



Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 Onwards

First Published: 2015-08-04

Last Modified: 2024-08-28

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I	Introduction	37
---------------	---------------------	-----------

CHAPTER 1	Read Me First	1
	Read Me First	1

CHAPTER 2	New and Changed Information	3
	New and Changed Information	3

PART II	CUBE Fundamentals and Basic Setup	7
----------------	--	----------

CHAPTER 3	Overview of Cisco Unified Border Element	9
	Overview	9
	SIP Trunking	11
	Deployment Scenarios	13
	Configure CUBE Features	14
	Enable the CUBE Application on a Device	15
	Verify CUBE on the Device	17
	Configure a Trusted IP Address List for Toll-Fraud Prevention	18

CHAPTER 4	Supported Platforms	21
	Supported Platforms	21
	Feature Comparison for Supported Platforms	23
	Virtual Cube	25
	Overview	25
	Feature Information	25
	Prerequisites	26

- Hardware 26
- Software 26
- Features Supported 27
- Virtual CUBE Support on Cisco CSR 1000V or C8000V Series Routers 27
 - vCUBE Licensing Requirements 27
- Installation 28
 - Install vCUBE on ESXi 28
 - Enable vCUBE 28
 - Troubleshoot vCUBE 29

CHAPTER 5

- Smart Licensing 31**
 - Overview 31
 - Smart License Operation 31
 - Smart Software Licensing Task Flow 33
 - Obtain the Registration ID Token 33
 - Configure Smart Licensing Transport Settings 33
 - Associate the Host Platform with CSSM 34
 - Configure CUBE Licensed Features 34
 - Verify Smart License Operation 35
 - High Availability Configurations 39
 - Smart Licensing with Box-to-Box High Availability 39
 - Verify Smart License Operation for Box-to-Box High Availability 40
 - Smart Licensing with Inbox High Availability 43
 - Verify Smart License Operation for Inbox High Availability 43
 - Syslog Messages 44

CHAPTER 6

- Configure Dial Peers 45**
 - Overview 45
 - Preferences 47
 - Configure Inbound and Outbound Dial-Peer Matching 48

CHAPTER 7

- DTMF Relay 51**
 - Overview 51
 - Feature Information 51

DTMF Tones	52
DTMF Relay	52
Interoperability and Priority with Multiple DTMF Relay Methods	55
DTMF Interoperability Table	55
Configure DTMF Relay	58
Verify DTMF Relay	58

CHAPTER 8**Introduction to Codecs 63**

Overview	63
Restrictions	64
Media Transmission	65
Voice Activity Detection	65
VoIP Bandwidth Requirements	66
Supported Audio and Video Codecs	68
Configure Codecs	69
Configure Voice Class Codec and Preference Lists	69
Configure Audio and Video Codecs at the Dial Peer Level	71
Verify an Audio Call	73
Configuration Examples for Codecs	73

CHAPTER 9**Call Admission Control 75**

Overview	75
Feature Information	75
Configure CAC Based on Total Calls, CPU or Memory	76
Example: Internal Error Code (IEC) for Default Call Rejection Based on CPU Utilization and Memory	77
Configure CAC Based on Call Spike Detection	77
Configure CAC Based on Maximum Calls per Destination	78
Bandwidth-Based Call Admission Control	79
Maximum Bandwidth Calculation	80
Bandwidth Tables	80
Restrictions	82
Configure Bandwidth-Based Call Admission Control	82
Configure Bandwidth-Based Call Admission Control at the Interface Level	82

Configure Bandwidth-Based Call Admission Control at the Dial Peer Level 84

Configure the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping 85

Verify Bandwidth-Based Call Admission Control 87

Tips to Troubleshoot 89

Configuration Examples for Bandwidth-Based Call Admission Control 89

Example: Configuring Bandwidth-Based Call Admission Control at the Interface Level 89

Example: Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level 89

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level 90

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level 90

CHAPTER 10

SIP Binding 91

Overview 91

Feature Information 91

Benefits of SIP Binding 92

Source Address 92

Voice Media Stream Processing 94

Configure SIP Binding 97

Verify SIP Binding 99

CHAPTER 11

Media Path 105

Overview 105

Feature Information 107

Configure Media Flow-Through 107

Configure Media Flow-Around 108

Configure Media Anti-Tromboning 109

CHAPTER 12

SIP Trunk Monitoring 111

Overview 111

Feature Information 112

OPTIONS Ping for DNS SRV Hosts 112

Load Balancing for DNS SRV Hosts 114

Configure SIP Out-of-Dialog OPTIONS Ping Group 114

Configuration Examples For SIP Out-of-Dialog OPTIONS Ping Group	116
Configure OPTIONS Ping Between CUCM and CUBE	118
Additional References	123

CHAPTER 13**VoIP for IPv6 125**

Overview	125
Feature Information	125
IPv6 SIP Features	125
SIP Protocol Handling for VoIPv6	126
VoIPv6 Support	127
Prerequisites	131
Restrictions	131
Configure SIP for IPv6	131
Configure the Protocol Mode of the SIP Stack	131
RTCP Pass-Through	132
Configure IPv6	132
Configure the Source IPv6 Address of Signaling and Media Packets	133
Configure the Session Target	135
Configure SIP Register Support	136
Configure IP Toll Fraud	137

PART III**Call Control 139****CHAPTER 14****Configure Tcl IVR Applications 141**

Overview	141
Tcl IVR Enhancements	142
TCL IVR Prompts Played on IP Call Legs	142
TCL Verbs	143
Prerequisites	145
TCL IVR Configuration Tasks	146
Configure the Call Application for the Dial Peer	146
Configure TCL IVR on the Inbound VoIP Dial Peer	148
Verify TCL IVR Configuration	150
TCL IVR Configuration Examples	152

CHAPTER 15 [Advanced Features for Cisco Contact Center](#) 153

- [Overview](#) 153
- [Feature Information Survivability.tcl Script for Contact Center](#) 153
- [Restrictions](#) 154

PART IV [Call Routing](#) 155

CHAPTER 16 [Configure and Troubleshoot DNS Resolution](#) 157

- [Overview](#) 157
- [Feature Information](#) 157
- [DNS Record Type](#) 158
- [Select the SRV Format Version](#) 158
- [Load Balance Among SRV Records](#) 159
- [Configure SRV Records](#) 160
- [Configure A and AAAA Records](#) 160
- [DNS Queries with VRF Configuration](#) 160
- [Verify the DNS Configuration on CUBE](#) 161
- [Troubleshoot DNS Configuration](#) 161

CHAPTER 17 [Matching Inbound Dial Peers by URI of Incoming SIP Calls](#) 163

- [Inbound Dial Peer Matching \(by URI\)](#) 163
 - [Feature Information](#) 163
- [Configure an Inbound Dial Peer to Match on URI](#) 164
- [Examples for Configuring an Inbound Dial Peer to Match on a URI](#) 166

CHAPTER 18 [URI-Based Dialing Enhancements](#) 169

- [Overview](#) 169
 - [Feature Information](#) 170
 - [Call Flows for URI-Based Dialing Enhancements](#) 170
- [Configure URI Dialing](#) 173
 - [Configure Pass Through of SIP URI Headers](#) 173
 - [Configure Pass Through of Request URI and To Header URI \(Global Level\)](#) 173
 - [Configure Pass Through of Request URI and to Header URI \(Dial Peer Level\)](#) 174

Configure Pass Through of 302 Contact Header	175
Configure Pass Through of 302 Contact Header (Global Level)	175
Configure Pass Through of 302 Contact Header (Dial Peer Level)	176
Derive the Session Target from URI	178
Example: Deriving Session Target from URI	180
Example: Configuring Pass Through of Request URI and To Header URI	180
Example: Configuring Pass Through of Request URI and To Header URI (Global Level)	180
Example: Configuring Pass Through of Request URI and To Header URI (Dial Peer Level)	180
Example: Configuring Pass Through of 302 Contact Header	180
Example: Configuring Pass Through of 302 Contact Header (Global Level)	180
Example: Configuring Pass Through of 302 Contact Header (Dial Peer Level)	181
Configuration Examples for URI-Based Dialing Enhancements	181
Example: Deriving Session Target from URI	181
Additional References for URI-Based Dialing Enhancements	181

CHAPTER 19**Multiple Pattern Support on a Voice Dial Peer 183**

Overview	183
Feature Information for Multiple Pattern Support on a Voice Dial Peer	183
Restrictions for Multiple Pattern Support on a Voice Dial Peer	184
Configure Multiple Pattern Support	184
Verify Multiple Pattern Support	186
Configuration Examples for Multiple Pattern Support	187

CHAPTER 20**Outbound Dial Peer Group as an Inbound Dial-Peer Destination 189**

Overview	189
Feature Information	189
Restrictions	190
Configure Outbound Dial-Peer Group as an Inbound Dial-Peer Destination	190
Verifying Outbound Dial-Peer Groups as an Inbound Dial-Peer Destination	193
Troubleshooting Tips	194
Configuration Examples for Outbound Dial Peer Group as an Inbound Dial-Peer Destination	195

CHAPTER 21**Inbound Leg Headers for Outbound Dial-Peer Matching 197**

Overview	197
----------	-----

- Feature Information 198
- Prerequisites for Inbound Leg Headers for Outbound Dial-PeerMatching 198
- Restrictions for Inbound Leg Headers for Outbound Dial-PeerMatching 198
- Configuring Inbound Leg Headers for Outbound Dial-PeerMatching 199
- Verify Inbound Leg Headers for Outbound Dial-PeerMatching 201
- Configuration Example: Inbound Leg Headers for Outbound Dial-Peer Matching 204

CHAPTER 22

Server Groups 207

- Overview 207
 - Feature Information for Configuring Server Groups in Outbound Dial Peers 208
- Configure Server Groups in Outbound Dial Peers 209
 - Configure Server Groups in Outbound Dial Peers 209
 - Verify Server Groups in Outbound Dial Peers 212
- Configuration Examples for Server Groups in Outbound Dial Peers 213

CHAPTER 23

Domain-Based Routing 217

- Overview 217
 - Feature Information 218
- Configure Domain-Based Routing 219
 - Configure Domain-Based Routing at Global Level 219
 - Configure Domain-Based Routing at Dial Peer Level 220
 - Verify and Troubleshoot Domain-Based Routing 220
- Configuration Examples for Domain-Based Routing 223
 - Example Configuring Domain-Based Routing 223

CHAPTER 24

ENUM Enhancement per Kaplan Draft RFC 225

- Overview 225
 - Feature Information for ENUM Enhancement per Kaplan Draft RFC 226
- Restrictions 226
- Configure ENUM 227
 - Enable Source-Based Routing 227
 - Test the ENUM Request 228
 - Verify the ENUM Request 228
- Troubleshooting Tips 229

Configuration Examples for ENUM Enhancement per Kaplan Draft RFC 230

PART V

SIP Header Manipulation 231

CHAPTER 25

Manipulate SIP Status-Line Header of SIP Responses 233

Manipulate SIP Status-Line Header of SIP Responses 233

Feature Information 233

Copy Incoming SIP Response Status Line to Outgoing SIP Response 234

Modify Status-Line Header of Outgoing SIP Response with User Defined Values 237

CHAPTER 26

Copy SIP Headers 239

Copy SIP Headers 239

Feature Information 239

Copy SIP Header Fields to Another 239

Copy From an Incoming Header and Modifying an Outgoing Header 239

Copy From One Outgoing Header to Another 242

Example: Copying the To Header into the SIP-Req-URI 243

CHAPTER 27

SIP Profiles 245

Overview 245

Feature Information 246

Important Characteristics of SIP Profiles 247

Restrictions 248

How to Configure SIP Profiles 249

Configure SIP Profile Rules Using Rule Tags 249

Upgrade or Downgrade SIP Profile Configurations 249

Configure a SIP Profile to Manipulate SIP Request or Response Headers 250

Processing Unsupported SDP Headers 252

Example: Configuring SIP Profile Rules (Attribute Passing) 254

Example: Configuring SIP Profile Rules (Parameter Passing) 254

Example: Configuration to Remove an Attribute 254

Use Non-standard SIP Headers in SIP Profiles 254

Configure a SIP Profile as an Outbound Profile 256

Configure a SIP Profile as an Inbound Profile 257

Supported SIP Messages 258

Verify SIP Profiles 262

Troubleshoot SIP Profiles 262

Examples: Adding, Modifying, Removing SIP Profiles 263

 Example: Adding a SIP, SDP, or Peer Header 263

 Example: Modifying a SIP, SDP, or Peer Header 264

 Example: Remove a SIP, SDP, or Peer Header 267

 Example: Inserting SIP Profile Rules 268

 Example: Upgrading and Downgrading SIP Profiles automatically 268

 Example: Modifying Diversion Headers 269

 Example: Sample SIP Profile Application on SIP Invite Message 270

 Example: Sample SIP Profile for Non-Standard SIP Headers 271

 Example: Copy User-to-User Information from REFER Message 271

CHAPTER 28

Pass Unsupported SIP Headers 273

Overview 273

 Feature Information 273

 Prerequisites 274

 Restrictions 274

Supported SIP Headers 274

Unsupported Headers 275

Enable Configurable Pass-Through of SIP INVITE Parameters (Global Level) 275

 Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Global Level) 276

Enable Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level) 276

 Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level) 277

Configure a Route String Header Pass-Through Using Pass-Through List 278

 Example: Configuring a Route String Header Pass-Through Using Pass-Through List 279

 Example: Passing a Header Not Supported by CUBE 280

PART VI

Protocol Interworking 281

CHAPTER 29

Basic SIP Configuration 283

Overview 283

 SIP Register Support 283

SIP Configuration Fundamentals	284
Configure SIP VoIP Services on a CUBE Gateway	284
Shut Down or Enable VoIP Service on CUBE Gateways	284
Shut Down or Enable VoIP Submodes on Cisco Gateways	285
Configure SIP Register Support	286
Configure SIP Redirect Processing	287
Configure Call-Redirect Processing	287
Configure SIP Implementation	289
Interaction with Forking Proxies	290
SIP Intra-Gateway Hairpinning	290
Verify CUBE Status	291
Tips to Troubleshoot	295
Configuration Examples	297
SIP Register Support Example	297
SIP 300 Multiple Choice Messages Example	299
Toll Fraud Prevention	301
<hr/>	
CHAPTER 30	Configurable SIP Parameters via DHCP 303
Overview	303
Feature Information	307
Prerequisites	307
Restrictions for Configurable SIP Parameters via DHCP	307
Configure SIP Parameters via DHCP	308
Configure the DHCP Client	308
Example: Configure the DHCP Client	309
Enable the SIP Configuration	310
Enable the SIP Configuration Example	311
Tips to Troubleshoot	311
Configure a SIP Outbound Proxy Server	312
Configure a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode	312
Configure a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode Example	313
Configure a SIP Outbound Proxy Server and Session Target in Dial Peer Configuration Mode	313
Configure a SIP Outbound Proxy Server in Dial Peer Configuration Mode Example	314

CHAPTER 31	Delayed Offer to Early Offer	317
	Delayed-Offer to Early-Offer	317
	Feature Information	317
	Delayed-Offer to Early-Offer in Media Flow-Around Calls	317
	Prerequisites for Delayed-Offer to Early-Offer	318
	Restrictions	318
	Configure Delayed Offer to Early Offer	318
	Configure Delayed Offer to Early Offer for Video Calls	319
	Configure Delayed Offer to Early Offer Medial Flow-Around	321
	MidCall Renegotiation Support for Delayed-Offer to Early-Offer Calls	322
	Restrictions for MidCall Renegotiation Support for DO-EO Calls	323
	Configure Mid Call Renegotiation Support for Delayed-Offer to Early-Offer Calls	323

CHAPTER 32	SIP: RFC 2782 Compliance with DNS SRV Queries	325
	Overview	325
	Feature Information	325
	SIP RFC 2782 Compliance with DNS SRV Queries	326
	Configure DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries	326
	Configure DNS Server Lookups	327
	Verifying	328

CHAPTER 33	Mid-call Signaling	331
	Overview	331
	Feature Information	331
	Prerequisites	332
	Mid-call Signaling Passthrough - Media Change	333
	Restrictions	333
	Behavior of Mid-call Re-INVITE Consumption	333
	Configure Passthrough of Mid-call Signalling	335
	Example Configuring Passthrough SIP Messages at Dial Peer Level	336
	Example Configuring Passthrough SIP Messages at the Global Level	336
	Mid-call Signaling Block	336
	Restrictions	337

Blocking Mid-Call Signaling	337
Example Blocking SIP Messages at Dial Peer Level	338
Example: Blocking SIP Messages at the Global Level	338
Mid Call Codec Preservation	339
Configure Mid Call Codec Preservation	339
Example: Configuring Mid Call Codec Preservation at the Dial Peer Level	340
Example: Configuring Mid Call Codec Preservation at the Global Level	340

CHAPTER 34**Early Dialog UPDATE Block 341**

Overview	341
Feature Information	341
Important Characteristics of Early Dialog UPDATE Block	342
Prerequisites	343
Restrictions	343
Configure Early Dialog UPDATE Block	343
Configure Early Dialog UPDATE Block Renegotiate	344
Tips to Troubleshoot	345

CHAPTER 35**Forked 18x Responses 347**

Overview	347
Feature Information for Consumption of Multiple Forked 18x Responses with SDP During Early Dialog	347
Characteristics of Forked 18x Responses with SDP during Early Dialog	348
Prerequisites	348
Restrictions	349
Configure Consumption of Forked 18x Responses with SDP During Early Dialog	349
Configure Consumption of Forked 18x Responses with SDP During Early Dialog Renegotiate	350
Tips to Troubleshoot	351

CHAPTER 36**Pass-Through of Unsupported Content Types in SIP INFO Messages 353**

Overview	353
Feature Information	354
Configure to Pass-through All Unsupported Content Types in a SIP INFO Messages	354

CHAPTER 37	Support for PAID, PPID, Privacy, PCPID, and PAURI Headers	355
	Overview	355
	Feature Information	365
	Restrictions	365
	Configure P-Header and Random-Contact Support	366
	Configure P-Header Translation	366
	Configure P-Header Translation on an Individual Dial Peer	367
	Configure P-Called-Party-Id Support	368
	Configure P-Called-Party-Id Support on an Individual Dial Peer	369
	Configure Privacy Support on a Cisco Unified Border Element	370
	Configure Privacy Support on an Individual Dial Peer	371
	Configure Random-Contact Support on a Cisco Unified Border Element	372
	Configure Random-Contact Support for an Individual Dial Peer	374

CHAPTER 38	Dynamic REFER Handling	377
	Dynamic Refer Handling	377
	Feature Information	377
	Prerequisites	378
	Restrictions	378
	Configure REFER Passthrough with Unmodified Refer-To	378
	REFER Handling - Delayed Disconnect	380
	Configure REFER Consumption	381
	Troubleshooting Tips	383

CHAPTER 39	Cause Code Mapping	385
	Overview	385
	Feature Information	385
	Cause Code Mapping	386
	Configure Cause Code Mapping	387
	Verify Cause Code Mapping	388

PART VII	Media Services	391
-----------------	-----------------------	------------

CHAPTER 40	Codec Support and Restrictions	393
	Overview	393
	Feature Information	393
	OPUS Codec	394
	Opus Codec Configuration	394
	Restrictions	396
	ISAC Codec Support on CUBE	396
	Restrictions	396
	AAC-LD MP4A-LATM Codec Support	396
	Restrictions for AAC-LD MP4A-LATM Codec Support	397
CHAPTER 41	Codec Preference Lists	399
	Overview	399
	Feature Information	399
	Codecs Configured Using Preference Lists	400
	Restrictions	400
	Configure Audio Codecs Using a Codec Voice Class and Preference Lists	401
	Disable Codec Filtering	402
	Troubleshoot Negotiation of an Audio Codec from a List of Codecs	403
	Verify Negotiation of an Audio Codec from a List of Codecs	404
CHAPTER 42	Payload Type Interoperability	407
	Overview	407
	Feature Information	407
	Restrictions	408
	Symmetric and Asymmetric Calls	408
	High Availability Checkpointing Support for Asymmetric Payload	409
	Configure Dynamic Payload Type Passthrough for DTMF and Codec Packets for SIP-to-SIP Calls	409
	Configure Dynamic Payload Type Passthrough at the Global Level	409
	Configure Dynamic Payload Type Passthrough for a Dial Peer	410
	Verify Dynamic Payload Interworking for DTMF and Codec Packets Support	411
	Tips to Troubleshoot	412
	Configuration Examples for Assymmetric Payload Interworking	413

Example: Asymmetric Payload Interworking—Passthrough Configuration 413
 Example: Asymmetric Payload Interworking—Interworking Configuration 413

CHAPTER 43

Transcoding Configuration 415
 Overview 415
 Configure LTI-Based Transcoding 416
 Configuration Examples for LTI Based Transcoding 417
 Verify Configuration 418
 VoIP Trace Logging 418

CHAPTER 44

Transrating Configuration 419
 Transrating 419
 Voice Packetization 419
 Configure Transrating for a Codec 420

CHAPTER 45

Call Progress Analysis 421
 Call Progress Analysis Over IP-to-IP Media Session 421
 Call Progress Analysis 421
 CPA Events 422
 Feature Information for Call Progress Analysis Over IP-IP Media Session 422
 Restrictions for Call Progress Analysis Over IP-to-IP Media Session 423
 Configure Call Progress Analysis Over IP-to-IP Media Session 424
 Enable CPA and Setting the CPA Parameters 424
 Example: Enabling CPA and Setting the CPA Parameters 425
 Verify the Call Progress Analysis Over IP-to-IP Media Session 426
 Tips to Troubleshoot 427

CHAPTER 46

Fax Detection 429
 Overview 429
 Feature Information for Fax Detection for SIP Call and Transfer 429
 Restrictions for Fax Detection for SIP Call and Transfer on Cisco IOS XE 430
 Information About Fax Detection for SIP Call and Transfer 430
 Local Redirect Mode 431
 Refer Redirect Mode 432

Fax Detection with Cisco IOS XE High Availability	433
Fax Detection Configuration for SIP Calls	433
Configure DSP Resource to Detect Fax Tone	433
Dial-peer Configuration to Redirect Fax Call	434
Verify Fax Detection Configuration for SIP Calls	436
Troubleshoot Fax Failures due to Multiple M-Lines on the CUBE	437
Fax Detection Troubleshooting for SIP Calls	438
Configuration Examples for Fax Detection for SIP Calls	439
Example: Configuring Local Redirect	439
Example: Configuring Refer Redirect	440

CHAPTER 47**Video Suppression** 441

Video Suppression	441
Feature Information for Video Suppression	441
Restrictions	442
Information About Video Suppression	442
Feature Behavior	442
Configuring Video Suppression	442
Troubleshooting Tips	443

CHAPTER 48**ICE-Lite Support** 445

ICE-Lite Support on CUBE	445
Feature Information	445
Characteristics	446
ICE Candidate	446
ICE Lite	447
High Availability Support with ICE	447
Restrictions for ICE-lite Support	447
Configure ICE-Lite	448
Verify ICE-Lite (Success Flow Calls)	449
Error Flow Calls	452
Configuration Example	457
Troubleshoot ICE-Lite Support	457
Additional References	458

CHAPTER 49	NAT Traversal using RTP Keepalive	459
	Information about NAT Traversal using Media Keepalives	459
	Feature Information	460
	Media Keepalive Characteristics	460
	Restrictions	461
	Configure NAT Traversal using Media Keepalive	461
	Configure NAT Media Keepalive at the Dial Peer Level	461
	Configure NAT Media Keepalive at the Tenant Level	462
	Configure NAT Media Keepalive at the Global Level	463
	Verify NAT Traversal using Media Keepalive Configuration	463
	Configuration Example	464

CHAPTER 50	Configure Report Generation	467
	Overview	467
	Feature Information	467
	Prerequisites	468
	Restrictions	468
	Configure RTCP Report Generation	468
	Troubleshooting Tips	469

PART VIII	Media Forking	471
------------------	----------------------	------------

CHAPTER 51	Dial-peer Based Recording	473
	Dial-peer Based Recording	473
	Feature Information	473
	Deployment Scenarios for CUBE-based Recording	473
	Open Recording Architecture	475
	Network Layer	475
	Capture and Media Processing Layer	475
	Application Layer	475
	Media Forking Topologies	476
	Media Forking with Cisco UCM	476
	Media Forking without Cisco UCM	476

SIP Recorder Interface	477
Metadata	477
Restrictions	477
Configure Dial-peer Recording	478
Configure Dial-peer Recording (with Media Profile Recorder)	478
Configure Dial-peer Recording (without Media Profile Recorder)	481
Verifying the Dial-peer Recording	483
Additional References for Network-Based Recording	498

CHAPTER 52**SIP Forking 499**

Overview	499
Feature Information	499
Deployment	500
Prerequisites for SIPREC Recording	501
Restrictions for SIPREC Recording	501
Configure SIPREC-Based Recording	502
Configure SIPREC-Based Recording (with Media Profile Recorder)	502
Configure SIPREC-Based Recording (without Media Profile Recorder)	505
Configuration Examples for SIPREC-based Recording	507
Example: Configuring SIPREC-based Recording with Media Profile Recorder	507
Example: Configuring SIPREC-based Recording without Media Profile Recorder	507
Validate SIPREC Functionality	508
Troubleshoot	509
Nonworking Scenarios	513
Configuration Example for Metadata Variations with Different Mid-call Flows	514
Example: Complete SIP Recording Metadata Information Sent in INVITE or Re-INVITE	514
Example: Hold with Send-only / Recv-only Attribute in SDP	517
Example: Hold with Inactive Attribute in SDP	519
Example: Escalation	522
Example: De-escalation	524
Configuration Example for Metadata Variations with Different Transfer Flows	526
Example: Transfer of Re-INVITE/REFER Consume Scenario	526
Configuration Examples for Metadata Variations with Caller-ID UPDATE Flow	527
Example: Caller-ID UPDATE Request and Response Scenario	527

Configuration Example for Metadata Variations with Call Disconnect	528
Example: Disconnect while Sending Metadata with BYE	528

CHAPTER 53**Video Recording 531**

Overview	531
Feature Information	531
Full Intra-Frame Request	532
Configure Video Forking	532
Enabling FIR for Video Calls (Using RTCP of SIP INFO)	532
Configuring H.264 Packetization Mode	533
Monitoring Reference files or Intra Frames	534
Verify for Video Forking	535

CHAPTER 54**Third-Party GUID Capture 537**

Overview	537
Feature Information	537
Restrictions for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording	538
Configure Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording	538
Verify Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording	541
Configuration Examples for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording	542

CHAPTER 55**Network based Recording 543**

Overview	543
Feature Information	543
Extended Media Forking (XMF) Provider and XMF Connection	543
XMF Call-Based Media Forking	544
XMF Connection-Based Media Forking	545
Extended Media Forking API with Survivability TCL	545
Restrictions	546
Example of SDP Data sent in an SRTP Call	547
Crypto Tag	547
Example of SDP Data sent in an SRTP Call	548
Multiple XMF Applications and Recording Tone	548

Forking Preservation	550
Configure UC Gateway Services	551
Configure Cisco Unified Communication IOS Services on the Device	551
Configur the XMF Provider	554
Verify the UC Gateway Services	555
Tips to Troubleshoot	557
Example: Configuring UC Gateway Services	557
Example: Configuring Cisco Unified Communication IOS Services	558
Example: Configuring the XMF Provider	558
Example: Configuring UC Gateway Services	558

CHAPTER 56
Media Proxy and Recording 559

Overview	559
Feature Information	559
Supported Platforms	560
Restrictions	560
CUBE Media Proxy Using Unified CM Network-Based Recording	561
SIPREC-Based Media Proxy	561
About Multiple Media Forking Using CUBE Media Proxy	561
Secure Forking of Secure and Nonsecure Calls	562
Deployment Scenarios for Media Proxy	562
Media Proxy Using Unified CM Network-Based Recording	562
SIPREC-Based Media Proxy	564
Recording Metadata	564
Session Identifier	567
Session-ID Handling	567
Recording State Notification	568
SIP Info Messages from CUBE Media Proxy to Unified CM	568
SIP Info Message Sent During the Initial Call	570
Media Proxy Configuration	572
Configure Media Proxy for Network-Based Recording Solutions	572
Configure Outbound Dial-Peers to the Recorders	572
Configure Media Proxy	574
Configure SIPREC Media Proxy	577

- Verification of CUBE Media Proxy Configuration 578
- Supported Features 588
 - Mid-Call Message Handling 588
 - Secure Recording of Secure Calls and Nonsecure Calls 589
 - Support for High Availability 589
 - Media Latch 590

CHAPTER 57

- WebSocket-Based Media Forking for Cloud Speech Services 591**
 - Overview 591
 - Feature Information 593
 - Prerequisites 593
 - Benefits 594
 - Restrictions 594
 - Licensing for WebSockets in CUBE 595
 - License Usage 596
 - Feature Characteristics 597
 - Error Strings in WebSocket Forking 602
 - Configure WebSocket-Based Forking 603
 - Configure CA Signed Certificates for SIP TLS Support in WebSockets 606
 - Verify WebSocket-Based Forking 608

PART IX

Security 611

CHAPTER 58

- SIP TLS Support 613**
 - Overview 613
 - Feature Information 613
 - Deployment 614
 - Peer Verification 615
 - Remote Application Selection 616
 - TLS Cipher Suites 616
 - Restrictions 617
 - Prerequisites 617
 - Configure SIP TLS 617
 - Step 1: Create a certificate for CUBE to use 617

Step 1a: Create a private key	618
Step 1b: Create a trustpoint to hold the certificate	618
Step 1c: Create a certificate signing request	621
Step 1d: Authenticate the trustpoint using the signing CA's certificate	622
Step 1e: Import signed certificate	622
Step 2: Configure preferred TLS cipher options	622
Step 3: Configure TLS preferences with a TLS profile	623
Step 4: Configure trunk or Tenant for TLS	624
Configure SIP TLS (sip-ua)	625
Verify SIP TLS Configuration	627
Example: SIP TLS Configuration	629
Syslog Messages	630

CHAPTER 59**SRTP-SRTP Interworking 633**

Overview	633
Feature Information	634
Supplementary Services	635
Restrictions	636
Configure SRTP-SRTP Interworking	636
Configure SRTP	636
Configure Cipher Suite Preference (optional)	638
Apply Crypto Suite Selection Preference (optional)	639
Enable SRTP Fallback	641
Configuration Examples	644
Example: Configuring SRTP-SRTP Interworking	644
Example: Changing the Cipher-Suite Preference	646

CHAPTER 60**SRTP-RTP Internetworking 649**

Overview	649
Support for SRTP-RTP Interworking	649
Use SRTP-RTP Chain for Interworking Between AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80 Crypto Suites	651
Supplementary Services Support	652
Feature Information	652

- Prerequisites **653**
- Restrictions **653**
- Configure SRTP-RTP Interworking **653**
 - Example: SRTP-RTP Interworking **656**
- Configure Crypto Authentication **656**
 - Example: Configuring Crypto Authentication **657**
 - Example: Configuring Crypto Authentication (Dial Peer Level) **658**
 - Example: Configuring Crypto Authentication (Global Level) **658**
- Enable SRTP Fallback **658**
 - Troubleshooting Tips **660**
- Verify SRTP-RTP **661**

CHAPTER 61

- SRTP-SRTP Pass-Through** **663**
 - Overview **663**
 - Pass-Through of Unsupported Crypto Suites **663**
 - Feature Information **664**
 - Configure Pass-Through of Unsupported Crypto Suites for a Specific Dial Peer **664**
 - Configure Pass-Through of Unsupported Crypto Suites Globally **666**
 - Configuration Examples for SRTP-SRTP Pass-Through **667**

CHAPTER 62

- Monitoring of Phantom Packets** **669**
 - Overview **669**
 - Feature Information **670**
 - Restrictions **670**
 - Configure Monitoring of Phantom Packets **670**
 - Configuration Examples for Monitoring of Phantom Packets **672**
 - Additional References for Configurable Pass-Through of SIP INVITE Parameters **672**

CHAPTER 63

- Security Compliance** **675**
 - Overview **675**
 - Feature Information **676**
 - Supported Hardware and Software for Virtual CUBE **676**
 - Common Criteria Configuration on Cisco CSR 1000v and C8000v **676**
 - Enable Common Criteria Mode **676**

SIP TLS Configuration	677
SIP TLS Configuration Task Flow	677
Generate RSA Public Key	677
Configure Certificate Authority Server	678
Configure CSR Trustpoint	679
Configure Peer Trustpoint	680
Add Client Verification Trustpoint	681
Enforce Strict SRTP	682
HTTPS TLS Configuration	683
HTTPS TLS Configuration Task Flow	683
Prepare Cisco CSR 1000v Router's HTTP Server to Run in CC Mode	683
Create Certificate Map for HTTPS Peer Trustpoint	684
Configure HTTPS TLS Version	685
Configure Supported Cipher Suites	686
Apply Certificate Map to HTTPS Peer Trustpoint	686
NTP Configuration Restrictions in Common Criteria Mode	687
FIPS Configuration on Cisco CSR 1000v and C8000v	688
Configuration Requirements for FIPS Compliance	688

PART X
Configure Multiple Trunks Using Tenants 689

CHAPTER 64
Configure Multiple Trunks Using Tenants 691

Overview	691
Feature Information	695
Feature Characteristics of Configurable SIP Trunk Listen Port	695
Configure SIP Trunks using Voice Class Tenant	696
Example: Multiple Trunks using Registration with Tenants	698

CHAPTER 65
Support for Multi VRF 701

Overview	701
Feature Information	701
Information About Voice-VRF	702
Information About Multi-VRF	702
VRF Preference Order	703

- Restrictions 703
- Recommendations 704
- Configure VRF 704
 - Create a VRF 705
 - Assign Interface to VRF 706
 - Create Dial-peers 707
 - Bind Dial-peers 708
- Configure VRF Specific RTP Port Ranges 710
 - Example: VRF with overlapping and non-overlapping RTP Port Range 712
- Directory Number (DN) Overlap across Multiple-VRFs 713
 - Example: Associating Dial-peer Groups to Overcome DN Overlap 714
- IP Overlap with VRF 715
- Use Server Groups with VRF 717
- Inbound Dial-Peer Matching Based on Multi-VRF 718
 - Example: Inbound Dial-Peer Matching based on Multi-VRF 718
- VRF Aware DNS for SIP Calls 720
- High Availability with VRF 720
- Configuration Examples 721
 - Example: Configuring Multi-VRF in Standalone Mode 721
 - Example: Configuring RG Infra High Availability with VRF 725
- Troubleshooting Tips 731

PART XI

High Availability 733

CHAPTER 66

High Availability on Cisco 4000 Integrated Services Routers and Cisco Catalyst 8000 Series Edge Platforms 735

- Overview 735
 - Feature Information 736
 - Box-to-Box Redundancy 736
 - Redundancy Group (RG) Infrastructure 736
 - Network Topology 737
- Considerations and Restrictions 739
 - Considerations 739
 - Restrictions 740

Configure CUBE High Availability on Cisco 4000 Series ISR and Cisco Catalyst 8000 Series Edge Platforms	741
Prerequisites	741
Configure High Availability	742
Configuration Examples	747
Example: Control Interface Protocol Configuration	747
Example: Redundancy Group Protocol Configuration	747
Example: Redundant Traffic Interface Configuration	747
Verify Your Configuration	748
Tips to Troubleshoot	755

CHAPTER 67**High Availability on Cisco ASR 1000 and Cisco Catalyst 8000 Series Routers 757**

Feature Information	757
Overview	757
Inbox Redundancy	759
Box-to-Box Redundancy	759
Redundancy Group (RG) Infrastructure	759
PROTECTED Mode	760
Network Topology	760
Considerations and Restrictions	762
Considerations	762
Restrictions	764
Configure CUBE High Availability on Cisco ASR 1000 and Cisco Catalyst 8000 Series Routers	764
Before You Begin	764
Configure Inbox High Availability	765
Configure Box-to-Box High Availability	765
Configuration Examples	772
Verify Your Configuration	778
Verify Redundancy State on Active and Standby Routers	778
Verify Call State After Switchover	780
Verify SIP IP Address Bindings	783
Verify Current CPU Use	784
Force a Manual Failover for Testing	784
Tips to Troubleshoot	785

CHAPTER 68	High Availability on Cisco C8000V Series Cloud Services Routers	787
	Overview	787
	Feature Information	788
	Box-to-Box Redundancy	788
	Redundancy Group (RG) Infrastructure	788
	Network Topology	789
	Considerations and Restrictions	792
	Considerations	792
	Restrictions	793
	How to Configure vCUBE High Availability on C8000V Series Routers	794
	Prerequisite	794
	Configure High Availability	794
	Configuration Example	799
	Tips to Troubleshoot	800

CHAPTER 69	DSP High Availability Support	803
	DSP High Availability Support	803
	Feature Information	803
	Prerequisites for DSP High Availability	804
	Features Supported with DSP High Availability	804
	Restrictions for DSP High Availability	804
	Tips to Troubleshoot	805
	Configuration Examples for DSP HA	805

CHAPTER 70	Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices	807
	Overview	807
	Feature Information	808
	Call Escalation with Stateful Switchover	808
	Call De-escalation with Stateful Switchover	809
	Media Forking with High Availability	810
	Prerequisites for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices	810
	Restrictions for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices	811
	High Availability Protected Mode and Box-to-Box Redundancy for ASR	811

	Example: Configuring the Interfaces for ASR Devices	812
	Support for Box-to-Box High Availability with Virtual IP Addresses	812
	Monitor Call Escalation and De-escalation with Stateful Switchover	812
	Monitor Media Forking with High Availability	814
	Verify the High Availability Protected Mode	816
	Support for REFER and BYE/Also after Stateful Switch-Over	817
	Tips to Troubleshoot	818
	Example: Configuring SIP Binding	819
<hr/>		
CHAPTER 71	CVP Survivability TCL support with High Availability	821
	Overview	821
	Feature Information	821
	Prerequisites	822
	Restrictions	822
	Recommendations	822
	Configure CVP Survivability TCL support with High Availability	822
<hr/>		
PART XII	Cloud Services	823
<hr/>		
CHAPTER 72	Hosted Scenarios (Lineside Connectivity)	825
	Hosted and Cloud Services Delivery	825
<hr/>		
CHAPTER 73	Configure SIP Registration	827
	Overview	827
	Feature Information for SIP Registration Proxy	827
	Registration Pass-Through Modes	828
	End-to-End Mode	828
	Peer-to-Peer Mode	829
	Registration in Different Registrar Modes	830
	Registration Overload Protection	830
	Registration Overload Protection-Call Flow	831
	Registration Rate-limiting	831
	Registration Rate-limiting Success--Call Flow	831
	Prerequisites	832

Restrictions	832
Configure SIP Registration Proxy	832
Enable Local SIP Registrar	832
Configure SIP Registration Proxy at the Global Level	833
Configure SIP Registration Proxy at the Tenant Level	835
Configure SIP Registration Proxy at the Dial Peer Level	836
Configure Registration Overload Protection	838
Configure CUBE to Route a Call to the Registrar Endpoint	839
Verify the SIP Registration	840
Configuration Example—Hosted and Cloud Services SIP Registration Proxy	841

CHAPTER 74
Survivability Enhancements 843

Overview	843
Advantages of Using CUBE Survivability Feature	843
Local Fallback	843
Registration Synchronization	844
Registration Through Alias Mapping	844
CUBE Survivability When WAN is UP	845
CUBE Survivability When WAN Is Down	846
Feature Information for Survivability for Hosted and Cloud Services	848
Configure Survivability for Hosted and Cloud Services	848
Configure Local Fallback or Registration Synchronization Globally	848
Configure Local Fallback or Registration Synchronization at the Tenant Level	849
Configure Local Fallback or Registration Synchronization on a Dial Peer	851
Configuring Survivability for Phones Sending Single Register Request	851
Configure OPTIONS Ping	853
Configure Registration Timer	853
Configuring the REGISTER Message Throttling in CUBE	855
Configure the Class of Restrictions (COR) List	856
Verify Survivability	858
Configuration Examples—Survivability for Hosted and Cloud Services	860
Example: Configuring Local Fallback Globally	860
Example: Configuring Local Fallback at the Tenant Level	860
Example: Configuring Local Fallback on a Dial Peer	860

Example: Configuring Survivability for Phones Sending Single Register Request	860
Example: Configuring OPTIONS Ping	861
Example: Configuring the Registration Timer	861
Example: Configuring REGISTER Message Throttling	861
Example: Configuring the COR List	861

CHAPTER 75**SUBSCRIBE-NOTIFY Passthrough 863**

Overview	863
Feature Information	864
Restrictions	865
Information About SUBSCRIBE-NOTIFY Passthrough	865
SUBSCRIBE-NOTIFY Passthrough Request Routing	866
SUBSCRIBE-NOTIFY Passthrough Survivability Mode	866
Configure SUBSCRIBE-NOTIFY Passthrough	867
Configure an Event List	867
Configure SUBSCRIBE-NOTIFY Event Passthrough Globally	868
Configure SUBSCRIBE-NOTIFY Event Passthrough at the Dial-Peer Level	869
Verify SUBSCRIBE-NOTIFY Passthrough	869
Tips to Troubleshoot	871
Configuration Examples for SUBSCRIBE-NOTIFY Passthrough	872
Example: Configuring an Event List	872
Example: Configuring SUBSCRIBE-NOTIFY Event Passthrough Globally	872
Example: Configuring SUBSCRIBE-NOTIFY Event Passthrough under a Dial Peer	872

PART XIII**Serviceability 873****CHAPTER 76****VoIP Trace 875**

Overview	875
Feature Information	876
Prerequisites	877
Restrictions	877
Benefits of VoIP Trace	877
Guide to use VoIP Trace Framework	878
Configuration Example for VoIP Trace	879

Syslog Messages 882

CHAPTER 77**Session Identifier 883**

Overview 883

Feature Behavior 884

Feature Information 884

Configure Support for Session Identifier 885

Tips to Troubleshoot 885

CHAPTER 78**Call Quality Statistics 893**

Overview 893

Feature Information 894

Restrictions 895

Configure Call Quality Parameters 895

Configure Call Quality Criteria Parameters 895

Tips to Troubleshoot 896

Configuration Example for Call Quality Statistics 897

CHAPTER 79**Monitor Voice Quality 899**

Overview 899

VQM Metrics 900

Feature Information 900

Prerequisites 901

Restrictions 901

Configure Voice Quality Monitoring 902

Enable Media Statistics Globally 902

Example: Configuring Media Statistics Globally 903

Example: CDR Enabled MOS Output 903

Verify 903

Tips to Troubleshoot 905

CHAPTER 80**CDR Accounting 907**

Overview 907

CHAPTER 81**SNMP Accounting 909**Overview **909**Pass-Through of Unsupported Crypto Suites **909**Feature Information **910**



PART I

Introduction

- [Read Me First, on page 1](#)
- [New and Changed Information, on page 3](#)



CHAPTER 1

Read Me First

- [Read Me First, on page 1](#)

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Changed History

Changes	Description
Cisco IOS XE 17.15.1a	

Changes	Description
Resolved bugs for Cisco IOS XE Release 17.15.1a	<ul style="list-style-type: none"> • CSCwk11111 - Restriction while network-based recording, Music-on-Hold (MOH) is not recorded. • CSCwk31376 - Cisco 1100 Integrated Services Router (ISR) models ISR1100 4G/6G support CUBE features when running on IOS XE. • CSCwk36547 - Restriction for dial-peer group working only with valid E.164 patterns. • CSCwk42148 - List RFC 3264 An Offer or Answer Model with the Session Description Protocol (SDP) in the references. • CSCwk48467 - Restriction with a single call forking on a CUBE using both dial-peer based recording and SIPREC.

Obtaining Documentation and Submitting a Service Request

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 2

New and Changed Information

- [New and Changed Information](#), on page 3

New and Changed Information



Note

- For detailed information on CUBE features supported on Cisco IOS Releases, Cisco IOS XE 3S Releases, and Cisco IOS XE Amsterdam 17 Releases, refer to [CUBE Cisco IOS Feature Roadmap](#), [CUBE Cisco IOS-XE Feature Roadmap](#), and [CUBE Cisco IOS XE 17 Feature Roadmap](#) respectively.
- H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.
- For CUBE feature support information for Cisco IOS XE Bengaluru 17.5.1a and prior releases, see [Cisco Unified Border Element Configuration Guide](#).
- The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Description	Documented at
Cisco IOS XE 17.15.1a	
Secure SIP with TLS version 1.3 Support (recommended release)	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_sip_tls_support_cube.html
Cisco IOS XE 17.14.1a	
Secure SIP with TLS version 1.3 Support	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_sip_tls_support_cube.html

Description	Documented at
Cisco IOS XE 17.13.1a and Cisco IOS XE Dublin 17.12.2	
NAT Traversal using Media Keepalives	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m-nat-traversal-using-rtp-keepalives.html
Cisco IOS XE Dublin 17.12.1a	
IPv6 Flows in High Availability	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cube/config/ios-cube-high-avail.html https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cube/config/ios-cube-high-avail.html https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cube/config/ios-cube-high-avail.html
GCM Ciphers for WebSocket-Based Media Forking	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/websocket-forking-for-cube.html
Cover Buffer Enhancements for VoIP Trace	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m-voip-trace-for-cube.html
Cisco IOS XE Dublin 17.10.1a	
YANG model enhancements for CUBE	https://developer.cisco.com/docs/ios-xe-voip/ https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cube/config/ios-cube-high-avail.html
Cisco IOS XE Cupertino 17.9.1a	
Advanced Features for Cisco Contact Center	Overview, on page 153
OPTIONS Ping for DNS SRV Hosts	OPTIONS Ping for DNS SRV Hosts, on page 112
Load Balancing for DNS SRV Hosts	Load Balancing for DNS SRV Hosts, on page 114
Cisco IOS XE Cupertino 17.8.1a	
Configurable SIP listen port per trunk (tenant)	Configure SIP TLS, on page 617
Configurable TLS policy per trunk (tenant)	Configure SIP TLS, on page 617
mTLS Client CN-SAN validation	Overview, on page 613
Yang Models for mTLS	https://pubhub.cisco.com/detail/2289
Cisco IOS XE Cupertino 17.7.1a	
YANG Configuration Models for CUBE	https://pubhub.cisco.com/detail/2289 https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/sdwan-cr-book.html
Cisco IOS XE Bengaluru 17.6.2 and Cisco IOS XE Cupertino 17.7.1a	

Description	Documented at
Secure WebSocket-based Media Forking on Cisco 4431, 4451-X, and 4461 Integrated Services Routers	Overview, on page 591
Cisco IOS XE Bengaluru 17.6.1a	
Transcoding Support for OPUS Codec	Overview, on page 393
Web Socket-based media forking	Overview, on page 591



PART II

CUBE Fundamentals and Basic Setup

- [Overview of Cisco Unified Border Element, on page 9](#)
- [Supported Platforms, on page 21](#)
- [Smart Licensing, on page 31](#)
- [Configure Dial Peers, on page 45](#)
- [DTMF Relay, on page 51](#)
- [Introduction to Codecs, on page 63](#)
- [Call Admission Control, on page 75](#)
- [SIP Binding, on page 91](#)
- [Media Path, on page 105](#)
- [SIP Trunk Monitoring, on page 111](#)
- [VoIP for IPv6, on page 125](#)



CHAPTER 3

Overview of Cisco Unified Border Element

- [Overview, on page 9](#)
- [Configure CUBE Features, on page 14](#)

Overview

Cisco Unified Border Element (CUBE) bridges voice and video connectivity between two separate VoIP networks. It is similar to a traditional voice gateway, except for the replacement of physical voice trunks with IP-based voice trunks. Traditional gateways connect VoIP networks to telephone companies using a circuit-switched connection, such as PRI. The CUBE connects VoIP networks to other VoIP networks and enterprise networks to Internet telephony service providers (ITSPs).

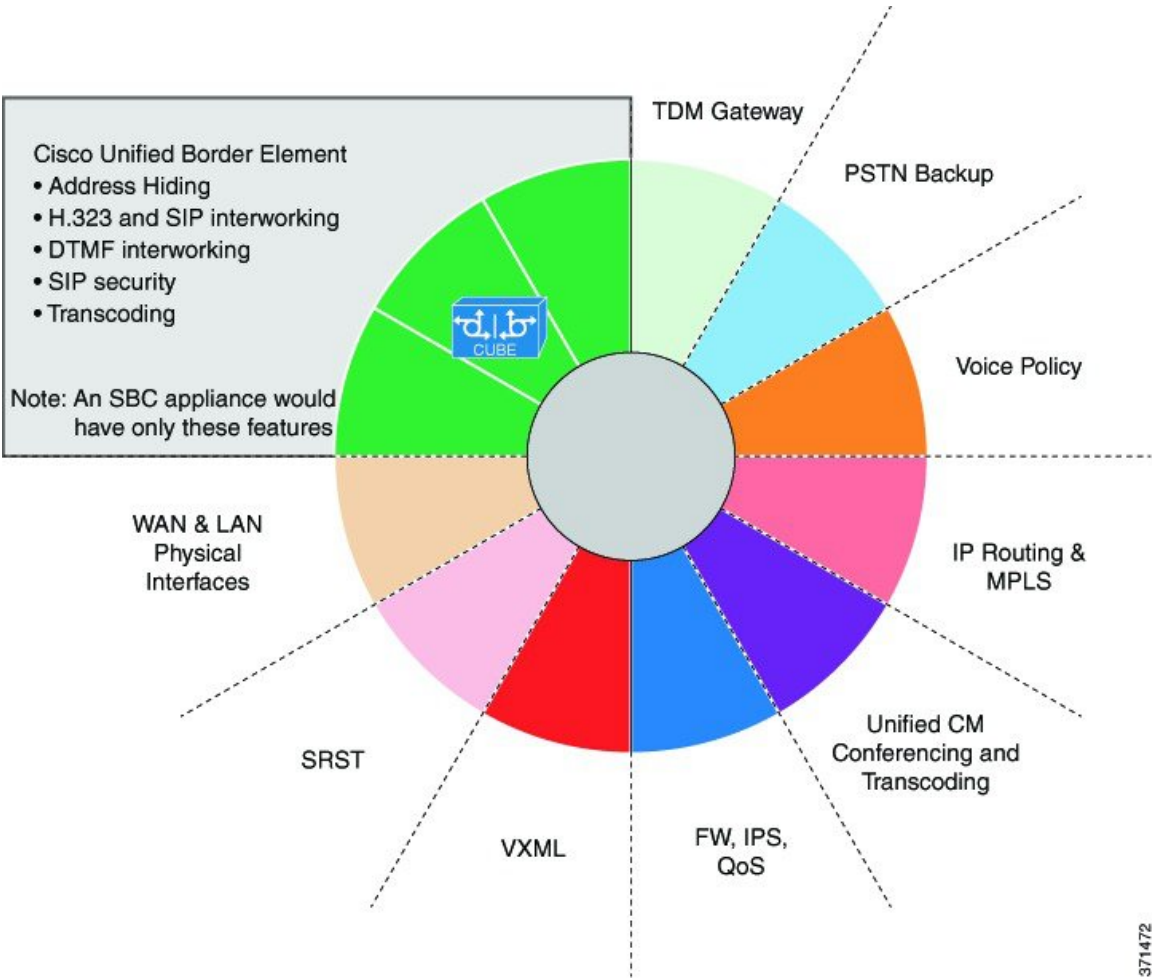
CUBE terminates and originates signaling Session Initiation Protocol [SIP] and media streams (Real-Time Transport Protocol [RTP] and RTP Control Protocol [RTCP]).



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

CUBE offers a wide variety of enhanced features in addition to the conventional Session Border Controller (SBC) functions as shown in the chart below:

Figure 1: CUBE—More Than an SBC



The CUBE provides a network-to-network interface point for:

- Signaling interworking SIP.
- Media interworking—Dual-tone multifrequency (DTMF), fax, modem, and codec transcoding.
- Address and Port translations—Privacy and topology hiding.
- Billing and call detail record (CDR) normalization.
- Quality-of-service (QoS) and bandwidth management—QoS marking using differentiated services code point (DSCP) or type of service (ToS), audio quality monitoring bandwidth enforcement using Resource Reservation Protocol (RSVP), and codec filtering.
- Media Forking—Replicate media packets for advanced media services such as call recording, transcription, and customer assist service in contact center environments.
- Media Proxy—Proxy "forked media" session to multiple recipients for policy compliance, redundancy, and advanced media services.
- Security Demarcation—Unencrypted signaling or media to encrypted signaling or media interworking.

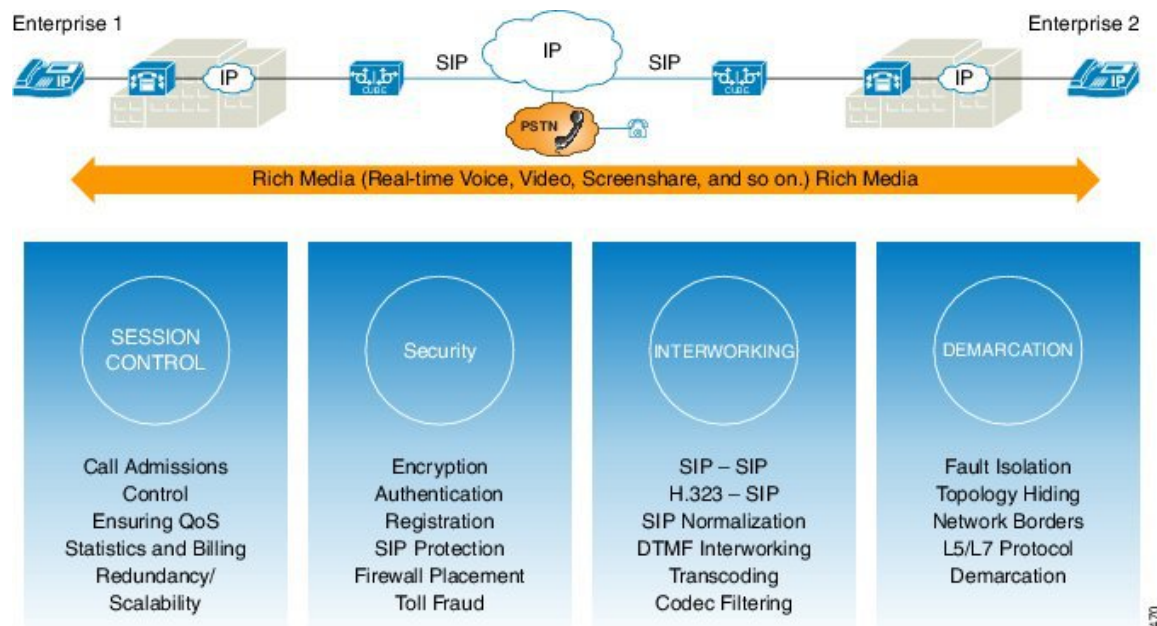
- Bridge enterprise and PSTN with cloud calling services such as Webex Calling, MS Teams Direct Routing and the like.

The CUBE provides a network-to-network demarcation interface for signaling interworking, media interworking, address and Port translations, billing, security, quality of service, call admission control, and bandwidth management.

The CUBE is used by enterprise and small and medium-sized organizations to interconnect SIP PSTN access with on-premise enterprise and hosted unified communications networks.

A CUBE interoperates with several different network elements including voice gateways, IP phones, and call-control servers in many different application environments, from advanced enterprise voice and video services with Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, as well as simpler toll bypass and VoIP (VoIP) transport applications. The CUBE provides organizations with all the border controller functions integrated into the network layer to interconnect unified communications voice and video enterprise-to-service-provider architectures.

Figure 2: Why Does an Enterprise Need the CUBE



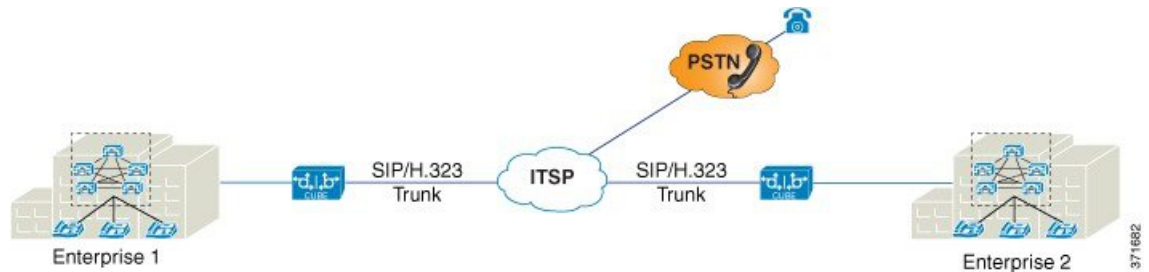
If enterprise subscribes to VoIP services offered by an ITSP, connecting the enterprise Cisco Unified Communications Manager through a CUBE provides network demarcation capabilities, such as security, topology hiding, transcoding, Call Admission Control, protocol normalization and SIP registration, none of which is possible if Cisco Unified Communications Manager connects directly to the ITSP. Another use case involves mergers or acquisitions in enterprise and the need to integrate voice equipment, such as CUCMs, IP PBXs, VM servers, and so on. If the networks in the two organizations have overlapping IP addresses, CUBE connects the two distinct networks until the acquired organization is migrated into the enterprise addressing plan.

SIP Trunking

The Session Initiation Protocol (SIP) is a signaling communications protocol, multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. SIP trunking is the use of VoIP

to facilitate the connection of Private Branch Exchange (PBX) to other VoIP endpoints across the Internet. To use SIP trunking, an enterprise must have a PBX (internal VoIP system) that connects to all internal end users, an Internet Telephony Service Provider (ITSP), and a gateway that serves as the interface between the PBX and the ITSP. One of the most significant advantages of SIP trunking is the ability to combine data, voice, and video in a single line, eliminating the need for separate physical media for each mode.

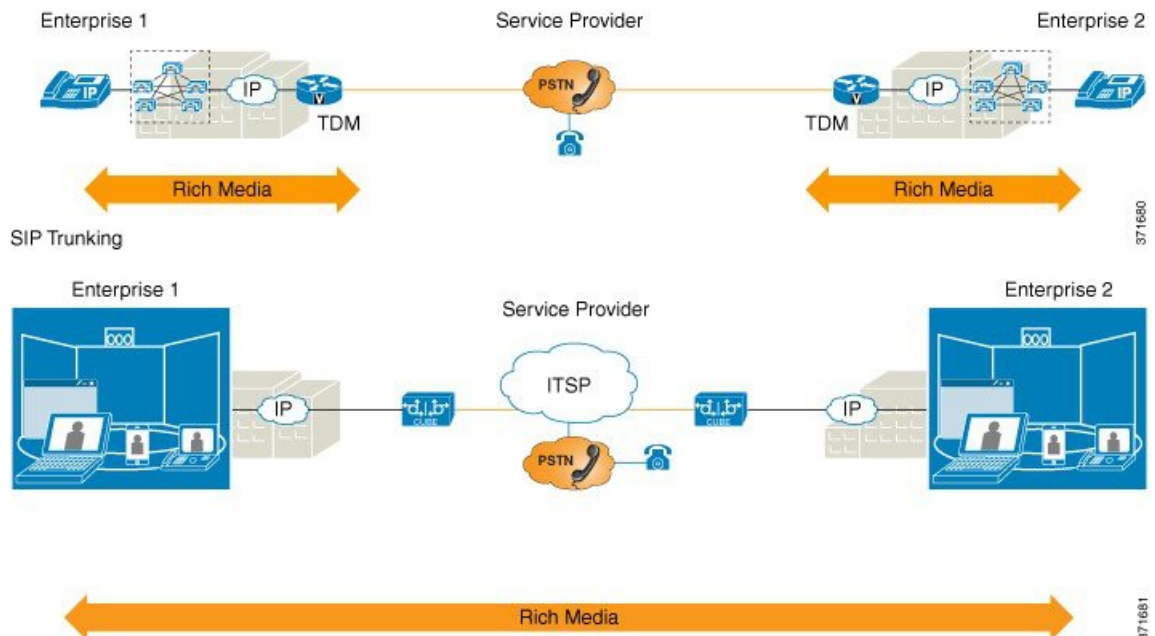
Figure 3: SIP Trunking



SIP trunking overcomes TDM barriers, in that it:

- Improves efficiency of interconnection between networks
- Simplifies PSTN interconnection with IP end-to-end
- Enables rich media services to employees, customers, and partners
- Carries converged voice, video, and data traffic

Figure 4: SIP Trunking Overcomes TDM Barriers





Note For Cisco IOS XE Gibraltar 16.11.1a and later releases, configure the either of the following CLIs to initiate the SIP processes:

- Voice dial-peer with **session protocol** as SIP.
- **voice register global**
- **sip-ua**

In the releases before Cisco IOS XE Gibraltar 16.11.1a, configure the following commands to initiate the SIP processes:

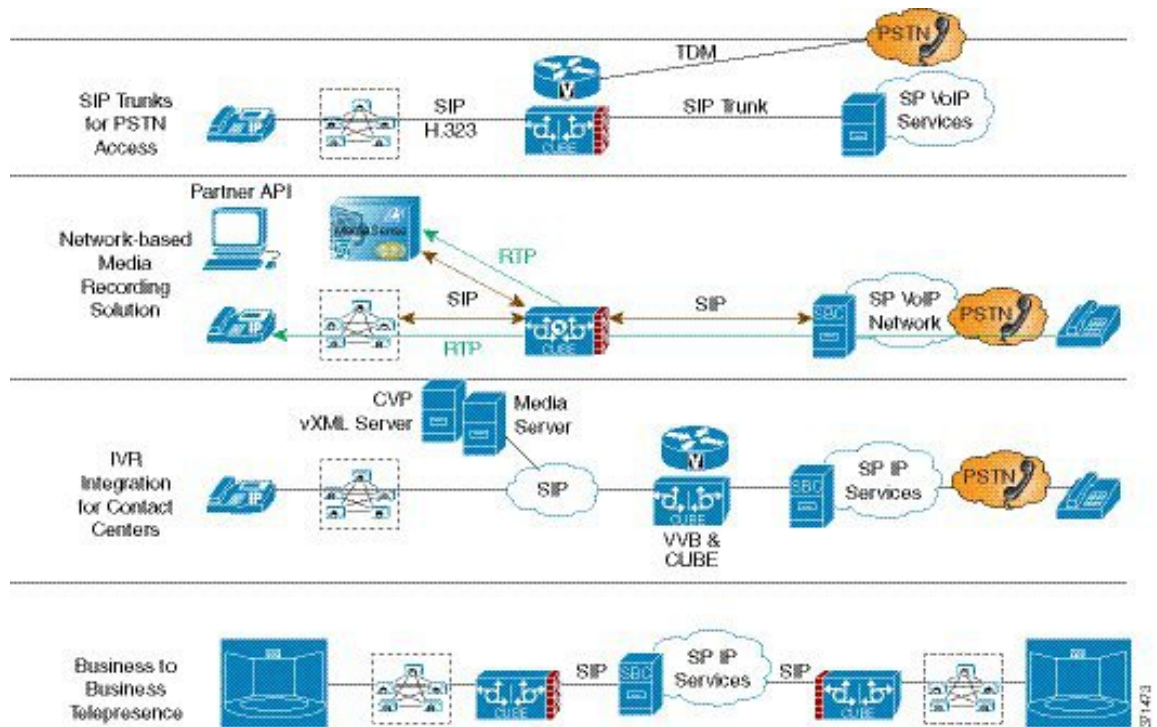
- **dial-peer voice** (*any*)
 - **ephone-dn**
 - **max-dn under call-manager-fallback**
 - **ds0-group 0 timeslots 1 type e&m-wink-start**
-

Deployment Scenarios

CUBE in an enterprise environment that serves:

- **PSTN Access:** Connect on-prem enterprise voice and hosted UC network via SIP trunks for PSTN calling services
- **Contact Center Integration:** Integration with contact center software components to provide inbound calling, outbound dialing, call queuing, IVR streaming, agent transfer, and advanced media forking services.
- **Webex Audio Edge:** Connect on-prem enterprise/PSTN to Webex Meetings (audio dial-in/dial-out).
- **Media Proxy/Forking**
- **Business-to-Business Telepresence**
- **Line side Registration Proxy**

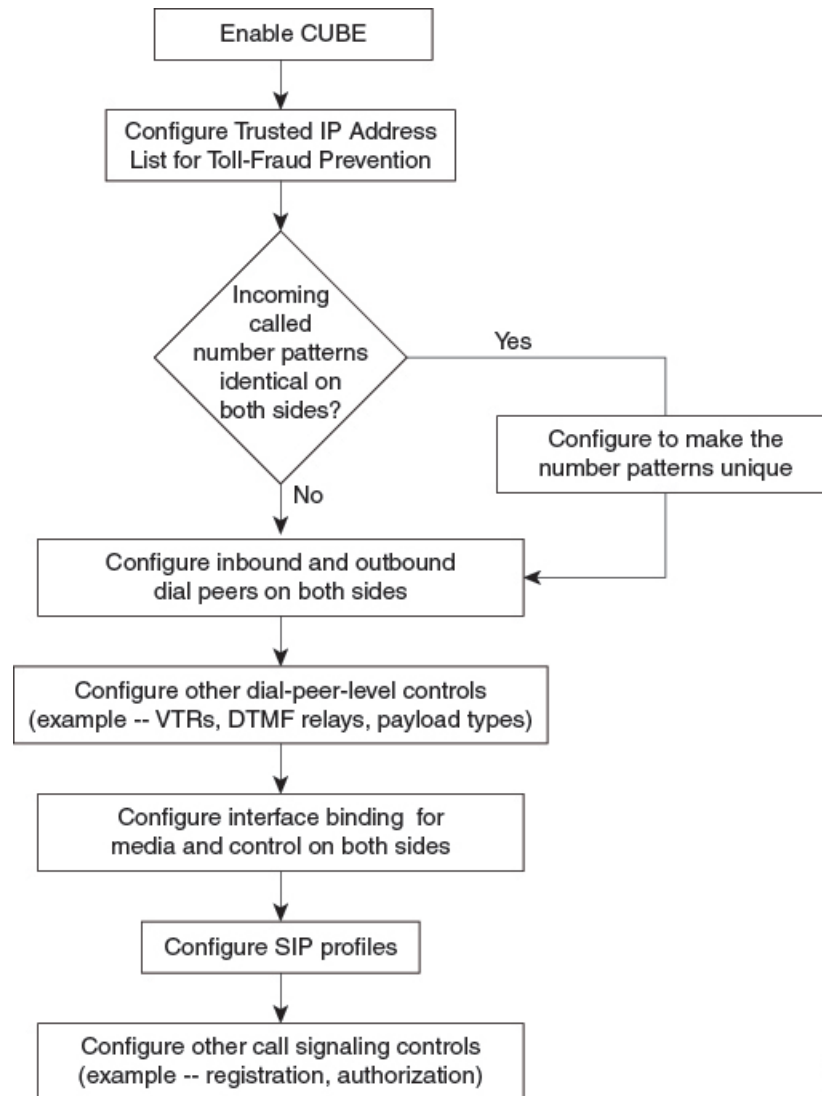
Figure 5: Typical Deployment Scenarios



Configure CUBE Features

Consider a scenario where XYZ corporation uses a VoIP network to provide phone services and uses a PRI connection for telecommunications services, and MGCP controls the PRI trunk. ITSP telecommunications provides migration from MGCP PRI to the SIP trunk. Cisco Unified Communications Manager (CUCM) sends the phone number, as 10 digits, to CUBE. CUCM sends only the extension (4 digits) to the CUBE. When the call is diverted (using call-forward), the requirement of the ITSP is that they need the full 10-digit number in the SIP Diversion field.

Figure 6: CUBE Configuration Workflow



The following sections describe the basic setup of CUBE through the steps that are involved in migrating the XYZ corporation to CUBE using a SIP trunk.

Enable the CUBE Application on a Device

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. mode border-element license [capacity *sessions* | periodicity {mins *value* | hours *value* | days *value*}]
5. allow-connections *from-type* to *to-type*
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters global VoIP configuration mode.
Step 4	mode border-element license [capacity <i>sessions</i> periodicity {mins <i>value</i> hours <i>value</i> days <i>value</i>}] Example: <pre>Device(conf-voi-serv)# mode border-element license capacity 200</pre> <pre>Device(conf-voi-serv)# mode border-element license periodicity days 15</pre>	<p>Enables CUBE configuration and configures the number of licenses (capacity).</p> <ul style="list-style-type: none"> Effective from Cisco IOS XE Amsterdam 17.2.1r, the capacity keyword and <i>sessions</i> argument are deprecated. However, the keyword and argument are available in the Command Line Interface (CLI). If you try to configure license capacity using CLI, the following error message is displayed: <div data-bbox="906 1140 1492 1268" style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>Error: CUBE SIP trunk licensing is now based on dynamic session counting. Static license capacity configuration has been deprecated.</pre> </div> Effective from Cisco IOS XE Amsterdam 17.2.1r, the periodicity keyword and [mins hours days] argument are introduced. The periodicity keyword configures periodicity interval for license entitlement requests for CUBE. If you do not configure license periodicity, the default license period of 7 days is enabled. <p>Note We recommend you to configure interval in days. Configuring interval in minutes or hours increases the frequency of entitlement requests and thereby increases the processing load on Cisco Smart Software Manager (CSSM). License periodicity configuration of minutes or hours is recommended to be used only with Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) mode.</p>

	Command or Action	Purpose
Step 5	allow-connections <i>from-type to to-type</i> Example: <pre>Device(conf-voi-serv)# allow-connections sip to sip</pre>	Allows connections between specific types of endpoints in a VoIP network. <ul style="list-style-type: none"> The two protocols (endpoints) refer to the VoIP protocols (SIP) on the two call legs.
Step 6	end Example: <pre>Device(conf-voi-serv)# end</pre>	Returns to privileged EXEC mode.

Verify CUBE on the Device

SUMMARY STEPS

1. **enable**
2. **show cube status**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show cube status

Displays the CUBE status, the software version, the license capacity, the image version, and the platform name of the device. In releases before , CUBE status display is enabled only if **mode border-element** command is configured with call license capacity. Effective from Cisco IOS XE Amsterdam 17.2.1r, this dependency is removed and Licensed-Capacity information is excluded from output.

Example:

Before Cisco IOS XE Amsterdam 17.2.1r:

```
Device# show cube status

CUBE-Version : 12.5.0
SW-Version : 16.11.1, Platform CSR1000V
HA-Type : none
Licensed-Capacity : 10
Calls blocked (Smart Licensing Not Configured) : 0
Calls blocked (Smart Licensing Eval Expired) : 0
```

Effective from Cisco IOS XE Amsterdam 17.2.1r:

```
Device# show cube status

CUBE-Version : 12.8.0
```

SW-Version : 17.2.1, Platform CSR1000V
 HA-Type : none

Configure a Trusted IP Address List for Toll-Fraud Prevention

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted list**
5. **ipv4 *ipv4-address* [*network-mask*]**
6. **ipv6 *ipv6-address***
7. **end**

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	voice service voip Example: Device(config)# voice service voip	Enters global VoIP configuration mode.
Step 4	ip address trusted list Example: Device(conf-voi-serv)# ip address trusted list	Enters IP address trusted list mode and enables the addition of valid IP addresses.
Step 5	ipv4 <i>ipv4-address</i> [<i>network-mask</i>] Example: Device(cfg-iptrust-list)# ipv4 192.0.2.1 255.255.255.0	Allows you to add up to 100 IPv4 addresses in the IP address trusted list. Duplicate IP addresses are not allowed. • The <i>network-mask</i> argument allows you to define a subnet IP address.
Step 6	ipv6 <i>ipv6-address</i> Example: Device(cfg-iptrust-list)# ipv6 2001:DB8:0:ABCD::1/48	Allows you to add IPv6 addresses to the trusted IP address list.

	Command or Action	Purpose
Step 7	end Example: Device(cfg-iptrust-list)# end	Returns to privileged EXEC mode.



CHAPTER 4

Supported Platforms

- [Supported Platforms, on page 21](#)
- [Feature Comparison for Supported Platforms , on page 23](#)
- [Virtual Cube, on page 25](#)

Supported Platforms



Note Cisco Cloud Services Router 1000V Series (CSR 1000V) is no longer supported from Cisco IOS XE Bengaluru 17.4.1a onwards. If you are using CSR 1000V, you have to upgrade to Cisco Catalyst 8000V Edge Software (Catalyst 8000V). For End-of-Life information on CSR 1000V, see [End-of-Sale and End-of-Life Announcement for the Select Cisco CSR 1000v Licenses](#).

Cisco Unified Border Element (CUBE) supports various platforms running on Cisco IOS XE Software Releases.



Note For information on migrating from existing Cisco IOS XE 3S releases to the Cisco IOS XE Denali 16.3 release, see [Cisco IOS XE Denali 16.3 Migration Guide for Access and Edge Routers](#).

The following table provides information on Cisco router platform support for CUBE:

Table 1: Supported Platforms

Cisco Router Platforms	Cisco Router Models	Cisco IOS Software Releases
Cisco 4000 Series-Integrated Services Routers (ISR G3)	Cisco 4321 Integrated Services Routers Cisco 4331 Integrated Services Routers Cisco 4351 Integrated Services Routers Cisco 4431 Integrated Services Routers Cisco 4451 Integrated Services Routers	Cisco IOS XE Denali 16.3.1 onwards
	Cisco 4461 Integrated Services Routers	Cisco IOS XE Amsterdam 17.2.1r onwards
Cisco 1000 Series-Integrated Services Routers (ISR)	Cisco 1100 Integrated Services Router series models ISR1100 4G/6G support CUBE features when running on IOS XE	Cisco IOS XE Gibraltar 16.12.1a onwards
Cisco Aggregated Services Routers (ASR)	Cisco ASR1001-X Aggregated Services Routers Cisco ASR1002-X Aggregated Services Routers Cisco ASR1004 Aggregated Services Routers with RP2 Cisco ASR1006 Aggregated Services Routers with RP2 and ESP40	Cisco IOS XE Denali 16.3.1 onwards
	Cisco ASR1006-X Aggregated Services Routers with RP2 and ESP40	Cisco IOS XE Fuji 16.6.1 onwards
	Cisco ASR1006-X Aggregated Services Routers with RP3 and ESP40/ESP100	Cisco IOS XE Everest 16.6.1 onwards
Cisco Cloud Services Routers (CSR)	Cisco Cloud Services Router 1000V series	Cisco IOS XE Denali 16.3.1 onwards
Cisco Cloud Services Routers (CSR)	Cisco Catalyst 8000V Edge Software (Catalyst 8000V)	Cisco IOS XE Bengaluru 17.4.1a onwards
Cisco 8300 Catalyst Edge Series Platforms	C8300-1N1S-6T C8300-1N1S-4T2X C8300-2N2S-6T C8300-2N2S-4T2X	Cisco IOS XE Amsterdam 17.3.2

Cisco Router Platforms	Cisco Router Models	Cisco IOS Software Releases
Cisco 8200 Catalyst Edge Series Platform	C8200-1N-4T	Cisco IOS XE Bengaluru 17.4.1a
Cisco C8200L Catalyst Edge Series Platform	C8200L-1N-4T	Cisco IOS XE Bengaluru 17.5.1a

Feature Comparison for Supported Platforms

The following table provides high level details of Cisco Unified Border Element (CUBE) features supported on different platforms.

Table 2: Feature Comparisons for Supported Platforms

Features	Cisco ASR 1000 Series Routers	Cisco ISR 4000 Series Routers	Cisco ISR 1000 Series Routers
High Availability Implementation	Redundancy Group Infrastructure	Redundancy Group Infrastructure	No
Media Forking	Yes (Cisco IOS XE Release 3.8S onwards)	Yes (Cisco IOS XE Release 3.10S onwards)	No
DSP Card Type	SPA-DSP	PVDM4 SM-X-PVDM	No
Transcoder registered to CUCM	No	Yes (Exists via SCCP - Cisco IOS XE Release 3.11S onwards)	No
Transcoder—LTI	Yes	Yes	No
Cisco UC Gateway Services API	Yes (Cisco IOS XE Release 3.8S onwards)	Yes	Yes
Noise Reduction and ASP	Yes	Yes	No
Call Progress Analysis	Yes (Cisco IOS XE Release 3.9S onwards ; Recommended - Cisco IOS XE Release 3.15S)	Yes Recommended - Cisco IOS XE Release 3.15S	No

Features	Cisco ASR 1000 Series Routers	Cisco ISR 4000 Series Routers	Cisco ISR 1000 Series Routers
SRTP-RTP Interworking	Yes - No DSP resources required (Cisco IOS XE Release 3.7S onwards)	Yes - No DSP resources required Cisco IOS XE Release 3.12S onwards	Yes - No DSP resources required
CUBE for SP Managed and Hosted Services	Yes	Yes	Yes
Unified SRST colocation with CUBE	Not supported	Yes (Cisco IOS XE Fuji 16.7.1 Release onwards)	Yes. From Cisco IOS XE Bengaluru 17.5.1a
IPv6	Yes	Yes	Yes

Table 3: Feature Comparisons for Supported Platforms (Contd...)

Features	Cisco CSR 1000V Series Routers	Cisco 8000V Catalyst Series Edge Platforms	Cisco 8300 Catalyst Edge Series Platforms	Cisco 8200 Catalyst Edge Series Platforms
HA Implementation	RG Infrastructure	RG Infrastructure	RG Infrastructure	RG Infrastructure
Media Forking	Yes	Yes	Yes	Yes
DSP Card Type	No	No	NIM-PVDM SM-X-PVDM	NIM-PVDM
Transcoder registered to CUCM	No	No	Yes (via SCCP)	Yes (via SCCP)
Transcoder—LTI	No	No	Yes	Yes
Cisco UC Gateway Services API	Yes	Yes	Yes	Yes
Noise Reduction & ASP	No	No	Yes	Yes
Call Progress Analysis	No	No	Yes	Yes
SRTP-RTP Interworking	Yes - No DSP resources required	Yes - No DSP resources required	Yes - No DSP resources required	Yes - No DSP resources required
CUBE for SP Managed and Hosted Services	Yes	Yes	Yes	Yes
Unified SRST colocation with CUBE	Not supported	No	Yes	Yes

Features	Cisco CSR 1000V Series Routers	Cisco 8000V Catalyst Series Edge Platforms	Cisco 8300 Catalyst Edge Series Platforms	Cisco 8200 Catalyst Edge Series Platforms
IPv6	Yes	Yes	Yes	Yes



Note For more information on Unified SRST and CUBE Co-location, see [Unified SRST and Unified Border Element Co-location](#).

Co-location of CUBE - High Availability (HA) with Unified SRST is not supported.

Virtual Cube

Overview

Virtual CUBE (vCUBE) is virtual deployment of Cisco Unified Border Element (CUBE) feature set.

From Cisco IOS XE Bengaluru 17.4.1a, vCUBE is available for use with Cisco® Catalyst® 8000V Edge Software (Catalyst 8000V) series.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 vCUBE Support

Feature Name	Releases	Feature Information
vCUBE in Microsoft Azure	Cisco IOS XE Bengaluru 17.6.3a	vCUBE offer is introduced in Microsoft Azure for Cisco Catalyst 8000V Edge Software (Catalyst 8000V).
vCUBE Catalyst 8000V Edge Software (Catalyst 8000V)	Cisco IOS XE Bengaluru 17.4.1a	vCUBE introduced for Cisco Catalyst 8000V Edge Software (Catalyst 8000V) in VMware ESXi environments and AWS environment.
vCUBE in Amazon Web Services (AWS)	Cisco IOS XE Gibraltar 16.12.4a	vCUBE offer introduced in AWS for Cisco CSR 1000v Series Cloud Services Router

Prerequisites

Hardware

- The vCUBE feature set is part of the Cisco virtual router software and is deployed in VMware ESXi virtualized environments. For more information on how to deploy Cisco virtualized routers in VMware ESXi environments, see [Install the Cisco CSR 1000V in VMware ESXi Environments](https://www.cisco.com/c/en/us/products/routers/catalyst-8000v-edge-software/index.html) and <https://www.cisco.com/c/en/us/products/routers/catalyst-8000v-edge-software/index.html>.
- For information on the best practices for setting ESXi host BIOS parameters for performance, see [BIOS Settings](#).
- Virtual CUBE is supported on the CSR 1000V and C8000V platforms.
- vCUBE is supported in AWS. You must use the AWS Marketplace product listing for virtual CUBE. For more information about the Cisco CSR 1000V and C8000V in AWS, see [Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services](#) and [Cisco C8000V Router Deployment Guide for Amazon Web Services](#).
- vCUBE is also supported in Microsoft Azure. You must use the Azure Marketplace product listing for virtual CUBE. For more information about C8000V in Microsoft Azure, see [Deploying Cisco Catalyst 8000V Edge Software on Microsoft Azure](#).



Note

- The CSR1000V and Catalyst 8000V products may be used in several different public and private cloud environments. However, vCUBE is only supported when deployed on VMware ESXi, AWS, and Microsoft Azure platforms currently.
- When you use a consolidated (.bin) image to upgrade a CSR 1000V medium configuration (2 vCPU, 4 GB RAM) to Catalyst 8000V, you must change the virtual machine vRAM allocation to at least 5 GB to ensure advertised performance. When deploying in AWS environments, boot the router using individual packages rather than a consolidated image without the need for extra memory. Refer to [Installing Subpackages from a Consolidated Package](#) for details.

Software

- Obtain the relevant license for the router platform. See [vCUBE Licensing Requirements](#), on page 27 for more information.
- In AWS platform, only Bring Your Own License (BYOL) is supported for vCUBE. Pay as You Go (Subscription) versions of the CSR 1000V and C8000V are not supported. Make sure you choose the vCUBE AWS Marketplace product listing. Refer to [Cisco Virtual CUBE-BYOL](#) for details.
- In Microsoft Azure platform, only Bring Your Own License (BYOL) is supported for vCUBE. Pay as You Go (Subscription) versions of the C8000V are not supported. Make sure you choose the vCUBE Azure Marketplace product listing. Refer to [Cisco Virtual CUBE-BYOL](#) for details.
- For more information about Cisco virtual routers, see [CSR 1000V Data Sheet](#) and [Catalyst 8000V Data Sheet](#).

Features Supported

vCUBE supports most of the CUBE features available in IOS XE releases.



Note From Cisco IOS XE Cupertino 17.8.1a onwards, Catalyst 8000V supports software MTP for Cisco Unified Communications Manager.

vCUBE does not support the following:

- DSP-based features
 - Codec Transcoding, Transrating
 - Raw in-band to RTP-NTE DTMF Interworking
 - Call Progress Analysis (CPA)
 - Noise Reduction (NR), Acoustic Shock Protection (ASP), and Audio Gain
 - IOS-based Hardware MTP



Note CUBE high availability is not supported on vCUBE when deployed in AWS and Microsoft Azure platforms.

Virtual CUBE Support on Cisco CSR 1000V or C8000V Series Routers

vCUBE media performance depends on the underlying host platform consistently providing packet switching latency of less than 5 milliseconds. The recommended hardware and virtual machine configurations ensure this performance when followed closely. For more information on how to monitor media performance, see [Voice Quality Monitoring](#).

vCUBE Licensing Requirements

vCUBE with CSR1000V

vCUBE is enabled for the CSR1000V with the APPX and AX platform licenses. vCUBE processes and CLI commands are enabled when either of these licenses are enabled. Secure call features require the AX license. In common with all CUBE instances, CUBE smart licenses are required for each active session.

The following table details the license requirements for vCUBE on the CSR1000V.

Virtual CUBE Session License	Platform License	Features	Throughput License
CUBE Smart Licenses	APPX	No TLS / SRTP support	Session count * (signaling + bidirectional media bandwidth)
	AX	All vCUBE features	

For detailed information about licensing, see [Cisco CSR 1000V Series cloud services Router Configuration Guide](#) and [Overview](#).

vCUBE with C8000V

vCUBE is enabled for the C8000V with the DNA Network Essentials with an appropriate bandwidth tier license.



Note When upgrading to C8000V software from a CSR1000V release, an existing throughput configuration is reset to a maximum of 250 Mbps. Install an HSEC authorization code, which you can obtain from your Smart License account, before reconfiguring your required throughput level.

Virtual CUBE Session License	DNA Subscription	Features	Bandwidth Tier License
CUBE Smart Licenses	Essentials or above	All vCUBE features	Session count * (signaling + media bandwidth)

For detailed information on licensing, see [Licensing](#).

Installation

You can install Virtual CUBE in two ways:

- Install using an OVA file
- Install using an ISO image

Install vCUBE on ESXi

Procedure

	Command or Action	Purpose
Step 1	Use the CSR1000V or the C8000V OVA application file (available from software.cisco.com) to deploy a new virtual instance directly in VMware ESXi.	<p>Note Select the required instance size during the OVA deployment.</p> <p>For further details on how to perform the deployment, see Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide or Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.</p>

Enable vCUBE

Procedure

	Command or Action	Purpose
Step 1	Power on the virtual machine.	
Step 2	Enable platform and throughput licenses and register to a Cisco licensing server.	

	Command or Action	Purpose
Step 3	Perform the steps Enable the CUBE Application on a Device to enable vCUBE.	

Troubleshoot vCUBE

To troubleshoot vCUBE, follow the same procedure as that of Cisco hardware routers. This includes crash file decoding, decoding traceback, and so on. For more details, see [Troubleshoot Cisco ASR 1000 Series Aggregation Services Routers Crashes](#).

To troubleshoot Virtual Machine (VM) issues, see [Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide](#) and [Cisco Catalyst 8000V Edge Software Configuration Guide](#).



CHAPTER 5

Smart Licensing

- [Overview, on page 31](#)
- [Smart License Operation, on page 31](#)
- [Smart Software Licensing Task Flow, on page 33](#)
- [Verify Smart License Operation, on page 35](#)
- [High Availability Configurations, on page 39](#)
- [Syslog Messages, on page 44](#)

Overview

Cisco Smart Licensing using Policy is a software licensing model that provides visibility of ownership and usage through the Cisco Smart Software Manager (CSSM) portal. CSSM is a central license repository that manages licenses across all Cisco products that you own, including CUBE. Devices send license usage to CSSM either directly or use an on-premises application. Your Smart Account Administrator controls your access to CSSM. Use your Cisco credentials to access the CSSM portal through <http://software.cisco.com>.

Smart Licensing applies to all platform technology (UCK9, Security, DNA) and CUBE feature licenses that the platform uses.

CSSM shows license usage across all devices that are registered to a virtual account. A Virtual Account License Inventory displays the quantity of licenses that are purchased, those licenses in use, and a balance. An **Insufficient Licenses** alert is displayed if the license balance is below 0.

For example, consider a smart account in CSSM with 50 CUBE trunk session licenses. If you have a single registered CUBE router using 20 trunk sessions, the CSSM licenses page shows **Purchased** as 50, **In Use** as 20, and **Balance** as 30.

For more information on Smart Software Manager, see the [Cisco Smart Software Manager User Guide](#).

Smart License Operation

Smart Licensing using Policy introduces a new paradigm for tracking license usage across your business. In earlier releases, license authorization was forward looking, binding licenses to a device until the next authorization request. Actual license use during the proceeding reporting period is now sent to CSSM, allowing you to plan ongoing license requirements based on historical usage data.

Each time a change in license usage is detected, the account policy defines how soon this should be reported to CSSM. Typically, this means that CUBE must send a report at least every 90 days, although it is

recommended that reports are sent more frequently. CSSM acknowledges each submitted Resource Utilization Monitoring (RUM) report to ensure that the use is recorded reliably. If the router does not receive an acknowledgment within the minimum reporting period, call processing may be disabled. Call processing is resumed when a valid acknowledgment is received.

Submit the reports to CSSM directly or through a Smart Software Manager On-Prem server. The Cisco Smart Licensing Utility (CSLU) application can also collect usage reports, providing more flexibility in managing your license usage. When a device is not able to communicate directly with a licensing server, a signed usage report can be generated and manually uploaded to CSSM. The acknowledgment that is generated by CSSM must be uploaded to the device within the license reporting policy period to ensure continued use.



Note CUBE_T_VGW records TDM license count when there is a TDM-SIP call. The **show license all** command displays the number of licenses that are used and is an expected behaviour. The CUBE_T_VGW is not displayed when there is no TDM-SIP call, and the CUBE does not act as a gateway. The TDM-SIP call service continues uninterrupted even if the device is not registered to CSSM or RUM acknowledgement is not received from the CSSM server.



Note Cisco Smart Software Manager On-Prem Version 8 Release 202102 or later is required for any device using SLP. Refer to the SLP feature documentation for further information ([Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#)).



Warning When using any of the following Smart Licensing using Policy releases, CUBE shuts down if the router does not receive a report acknowledgment from CSSM before the acknowledgment deadline set by the account policy: 17.3.2, 17.3.3, 17.3.4a, 17.6.1a, or any 17.4 or 17.5 release. CUBE does not shut down in this way with later releases.

License usage is calculated dynamically in the same way as earlier releases, with measurements recorded periodically based on the periodicity timer. Measurements are stored locally until they are submitted to CSSM. This historical usage reporting allows for more accurate aggregation of use across multiple devices over time. The minimum value for the periodicity timer is increased to 8 hours.

The system records the changes every eight hours. It reports these changes to CSSM as soon as it detects any variations from the previous value. However, note that this report is limited to a maximum frequency of once per 24 hours.

If the peak license usage for the current period is different by more or less than 25% of the previously reported value, it is reported and periodicity interval is reset. Use of CUBE Standard Trunk and CUBE Enhanced Trunk licenses are monitored separately.



Note Smart License Reservation (SLR) for CUBE licenses is not compatible with SLP. Even if a reservation is in place when upgrading, license use reporting will still be required in accordance with the device policy. Reservations should therefore be returned immediately before or after upgrading to a release that uses SLP.



Note From Cisco IOS XE Bengaluru 17.6.1a onwards, calls that are forked using WebSockets are marked as consuming an Enhanced session license.

Smart Software Licensing Task Flow

IOS XE license use reports may either be pushed to or pulled by a licensing server. Refer to the workflows in [Smart Licensing Using Policy for Cisco Enterprise routing Platforms](#) for more details.

Obtain the Registration ID Token

Detailed Steps

1. Log in to your Smart Account in either CSSM or satellite.
2. Navigate to the Virtual Account to register the CUBE.
3. Generate a registration ID token.

Configure Smart Licensing Transport Settings

Step 1 `hostname` *hostname*

Example:

```
Device(config)# hostname cube
cube(config)#
```

Ensure that hostname and the PID of the platform are not the same. For example, if the hostname of an ASR1006 router is configured as "ASR1006," registration is unsuccessful.

Step 2 `ip name-server` *IP Address*

Example:

```
cube(config)# ip name-server 10.0.0.1 10.0.0.10
```

Configures valid DNS servers to ensure the correct resolution of the CSSM hostname.

Step 3 `ip http client source-interface` *interface name*

Example:

```
cube(config)# ip http client source-interface GigabitEthernet0/0/0
```

Binds the platform HTTP client to the interface used to access the CSSM.

Step 4 `license smart transport smart`

Example:

```
cube(config)# license smart transport smart
```

Smart transport is the preferred method for sending usage reports.

Step 5 `license smart proxy address` *host-name***Example:**

```
cube(config)# license smart proxy address proxy.cisco.com
```

If necessary, configure a proxy-server for the platform when a direct HTTP connection to CSSM is not permitted.

Step 6 `license smart proxy port` *port-number***Example:**

```
cube(config)# license smart proxy port 80
```

If using an internet proxy, configure a proxy-server port number.

Step 7 `license smart url default`**Example:**

```
cube(config)# license smart url default
```

Use the default URL for sending reports to CSSM.

Associate the Host Platform with CSSM

From Cisco IOS XE Everest 16.11.1a to Cisco IOS XE Amsterdam 17.3.1a, you must register the host platform to either CSSM or SSM On-Prem to report license usage. From Cisco IOS XE Amsterdam 17.3.2 onwards, license use must be reported to CSSM or SSM On-Prem in accordance with the Smart Account reporting policy.

Before you begin

1. Obtain the registration ID token from your Smart Account.
2. Configure Smart Licensing transport settings.

Use the following command to register the CUBE platform with CSSM.

```
license smart trust id_token id_token...local [force]
```

Example:

```
Router# license smart trust id_token ZDEwZDFiODktNWF.....
```

Configure CUBE Licensed Features

Step 1 `voice service voip`**Example:**

```
Device(config)# voice service voip
```

Enters global VoIP configuration mode.

Step 2 `mode border-element [license periodicity {hours <8-23> | days <1-30> }]`

The periodicity keyword configures the CUBE measurement interval for license usage. If you do not configure the periodicity keyword, license usage is measured once every 7 days.

Verify Smart License Operation

This section shows CUBE license usage status and license usage history.

Use the following commands to verify the platform license usage:

- **show cube status**—Displays CUBE license status.

```
cube#show cube status
CUBE-Version : 14.4
SW-Version : 17.6.1a, Platform ISR4321/K9
HA-Type : none
```

- **show license status**—Displays the license policy and reporting status.



Note The acknowledgment deadline is presented in this output. Ensure that an acknowledgment is received before this time to ensure continued operation of the SIP service.

```
cube#show license status
Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Policy:
  Policy in use: Merged from multiple sources.
  Installed Time: Jan 01 05:30:00 1970 IST
  Reporting ACK required: yes
  Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (Product default)
  Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 80 (Product default)
  Enforced License Attributes:
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 80 (Customer Policy)
  Export License Attributes:
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
```

```

Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: May 26 08:24:45 2020 IST
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Jun 15 08:24:45 2020 IST
  Last report push: <none>
  Last report file write: <none>
  Last report pull: <none>

Trust Code Installed: <none>

```

- **show voice sip license stats**—Displays CUBE trunk license usage history.

License usage is recorded in tabular and graphical format for all the three types of trunk call count (Enhanced, Standard, and Aggregate). Usage is recorded based on the peak value of concurrent calls for a defined interval of time:

- **Seconds Table**—This table stores concurrent calls at every second for the last 60 seconds.
- **Minutes Table**—This table stores regularized peak value of concurrent calls at every minute for the last 60 minutes. Regularized peak for a minute is the average of top 3 peak values that occurs in a minute.
- **Hours Table**—This table stores peak value for each hour for the last 72 hours.
- **Days Table**—This table stores peak value for each day for the last 72 days.

The following example outputs are truncated to display 60-second and 60-minute tables only.

```

cube#show voice sip license stats table

02:50:16 PM Wednesday Nov 13 2019 UTC

```

```

CUBE Trunk License Usage (last 60 seconds)
Period      Average      Max
-----
1-5         0            0
6-10        0            0
11-15       0            0
16-20       0            0
21-25       0            0
26-30       0            0
31-35       0            0
36-40       0            0
41-45       0            0
46-50       0            0
51-55       0            0
56-60       0            0

```

```

CUBE Trunk License Usage (last 60 minutes)
Period      Average      Max
-----
1-5         0            0
6-10        0            0

```

```

11-15      0      0
16-20      0      0
21-25      0      0
26-30      0      0
31-35      0      0
36-40      0      0
41-45      0      0
46-50     324     900
51-55     343     899
56-60     292     600
    
```

```
cube#show voice sip license stats
```

```
11:01:01 AM Thursday Aug 29 2019 IST
```

```

10
 9
 8
 7
 6
 5
 4
 3
 2
 1
0....5....1....1....2....2....3....3....4....4....5....5....6
   0   5   0   5   0   5   0   5   0   5   0   5   0
CUBE Trunk License Usage (last 60 seconds)
    
```

```

910
820
730
640
550
460
370
280
190
100
 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   5   0
CUBE Trunk License Usage (last 60 minutes)
* = maximum      # = average
369863146641
8880900440044
3330922440011
**
#*
##
***  **
####  ##
##### *###*
*##### *###*
#####* #####
#####  #####
*#####*#####*
#####*#####*
    
```

- **show voice sip license status**—Displays the license status.

```
Router#show voice sip license status
Host Name: Router
```

```

Current Time: Mar 30 2021 00:32:35 UTC
SIP service: Up
License use recorded every: 8 Hour(s)
Next record at: Mar 30 2021 07:00:00 UTC
Recent use of license(s) for CUBE Standard Trunk
Verify Smart License Operation
-----

```

Timestamp Count

```

-----
Mar 29 2021 23:00:00 UTC 0
Mar 29 2021 22:00:00 UTC 9
Mar 29 2021 21:00:00 UTC 24
Mar 29 2021 20:00:00 UTC 13
Mar 29 2021 11:00:00 UTC 0
Mar 29 2021 09:00:00 UTC 2
Recent use of license(s) for CUBE Enhanced Trunk
-----

```

Timestamp Count

```

-----
Mar 29 2021 21:00:00 UTC 0
Mar 29 2021 20:00:00 UTC 2
Mar 29 2021 11:00:00 UTC 0
Mar 29 2021 09:00:00 UTC 8

```

- **show license usage**—Displays the license usage.

```

cube#show license usage
Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Policy:
  Policy in use: Merged from multiple sources.
  Installed Time: Jan 01 05:30:00 1970 IST
  Reporting ACK required: yes
  Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (Product default)
  Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 80 (Product default)
  Enforced License Attributes:
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 80 (Customer Policy)
  Export License Attributes:
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>

```



```

Next ACK deadline: May 26 08:24:45 2020 IST
Reporting Interval: 30
Next ACK push check: <none>
Next report push: Jun 15 08:24:45 2020 IST
Last report push: <none>
Last report file write: <none>
Last report pull: <none>

```

```
Trust Code Installed: <none>
```

- **show license summary**—Displays the license summary information.

```
Device#show license summary
```

```

License Usage:
License                Entitlement tag                Count  Status
-----
CUBE_T_STD              (CUBE_T_STD)                   5 IN USE
uclk9                  (ISR_4351_UnifiedCommun...)    1 IN USE
CUBE_T_VGW              (CUBE_T_VGW)                   4 IN USE

```

Commands Related to Smart License

- **show license all**—Displays all the information that is related to licensing.
- **show license tech support**—Displays the license technical support information.
- **show call-home smart-licensing**—Displays the destination URL that is configured.

Use the following commands to debug any issues that are related to your Smart License:

- **debug license feature cube all**

- Request successful for license_type:<license_type_int> and count <usage_count>.

Example:

```
*May 18 10:12:45.178: //CUBE-SL/Info/cube_sl_send_entitlement_request: Request
successful for license_type: 0 and count 9.
```

```
Request successful for license <license_type_string>
```

Example:

```
*May 18 10:15:45.181: //CUBE-SL/Info/cube_license_request: Request successful
for license CUBE_T_STD
```

High Availability Configurations

Smart Licensing with Box-to-Box High Availability

Box-to-Box redundancy uses the Redundancy Group (RG) Infrastructure to form High Availability (high availability) pair of platforms.

For Smart License configurations on the High Availability pair of platforms, see [Smart Software Licensing Task Flow, on page 33](#). When reporting license usage, the Smart Agent includes details of its high availability group and, if it is in the active or standby state. Thus allowing the CSSM to group license requirements for the high availability pair.

Box-to-Box High Availability requires CUBE Trunk Redundant Session licenses. From Cisco IOS XE Amsterdam 17.2.1r onwards, license usage is based on dynamic call counting.

Before Failover

- Establish a trust relationship for both platforms in the high availability configuration with the same CSSM Smart Virtual Account.
- CSSM sets the reporting policy for each platform.
- Only the active platform submits license usage reports to CSSM.

After Failover

- The platform that switches to the active mode reports license usage to the CSSM.
- The new active platform starts a new license measurement interval timer. For example, if a periodicity of five days is configured and failover occurs after three days, the next measurement will be recorded five days later.

Verify Smart License Operation for Box-to-Box High Availability

You can use all the commands that are given in the section [Verify Smart License Operation, on page 35](#) to verify the licensing status in High Availability mode. The following commands reflect Smart License information that is related to Box-to-Box high availability for IOS XE releases 16.11.1a:

The following commands reflect Box-to-Box high availability licensing information.

- **show cube status**—Displays CUBE license capacity and the high availability mode.

```
CSR#sh cube status
CUBE-Version : 14.4
SW-Version : 17.6.1a, Platform ISR4321/K9
HA-Type : hot-standby-chassis-to-chassis
```

- **show license usage**—Displays license usage.

```
CSR#sh license usage
License Authorization:
  Status: Not Applicable

CUBE_T_RED (CUBE_T_RED):
  Description: CUBE_T_RED
  Count: 100
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: CUBE_T_RED
  Feature Description: CUBE_T_RED
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

- **show license summary**—Displays the license summary information.

Following is the sample output from the active instance of CUBE.

```
CSR#sh license summary
License Usage:
  License                               Entitlement tag           Count Status
-----
  CUBE_T_RED                             (CUBE_T_RED)             1 IN USE
```

- **show license all**—Displays Active and Standby modes.

```
c8kv#sh license all
Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Apr 20 13:26:18 2021 UTC
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Oct 08 13:56:07 2021 UTC
  Next ACK deadline: Dec 07 13:56:07 2021 UTC
```

```

Reporting push interval: 1 days
Next ACK push check: Oct 22 20:44:57 2021 UTC
Next report push: Oct 23 16:24:52 2021 UTC
Last report push: Oct 22 16:24:52 2021 UTC
Last report file write: <none>

Trust Code Installed: Apr 20 13:26:18 2021 UTC

License Usage
=====

network-advantage_1G (ESR_P_1G_A):
  Description: network-advantage_1G
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_1G
  Feature Description: network-advantage_1G
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage_1G (DNA_P_1G_A):
  Description: dna-advantage_1G
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage_1G
  Feature Description: dna-advantage_1G
  Enforcement type: NOT ENFORCED
  License type: Subscription

CUBE_T_STD (CUBE_T_STD):
  Description: CUBE_T_STD
  Count: 121
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: CUBE_T_STD
  Feature Description: CUBE_T_STD
  Enforcement type: NOT ENFORCED
  License type: Perpetual

Product Information
=====
UDI: PID:C8000V,SN:93POM8FF9IZ

Agent Version
=====
Smart Agent for Licensing: 5.1.21_rel/96

License Authorizations
=====
Overall status:
  Active: PID:C8000V,SN:93POM8FF9IZ
    Status: SMART AUTHORIZATION INSTALLED on Sep 21 13:48:56 2021 UTC
    Last Confirmation code: 1fc54c75

Purchased Licenses:
  No Purchase Information Available#

```

Smart Licensing with Inbox High Availability

You can configure a Cisco ASR 1000 Series Router platform with two Route Processors for Inbox High Availability using Stateful Switchover (SSO). In this configuration, one Route Processor is active while the other is in standby mode.

For Smart License configuration, see [Smart Software Licensing Task Flow](#). Only the active Route Processor in the SSO configuration reports license usage, so CSSM reserves one set of licenses for the platform.

Inbox High Availability requires CUBE Trunk Standard Session licenses.

Before Failover

- Smart License configuration is synchronized between the two Route Processors. Only the active Route Processor registers with CSSM or satellite.
- The CSSM or satellite authorizes license usage requests for the active Route Processor.



Note For Smart License using Policy, the CSSM or satellite license usage requests for the active Route Processor.

After Failover

- The Route Processor that switches to active mode, reports license usage to the CSSM or satellite.
- As the new report appears to come from the same device, the CSSM or satellite retains the original reservation for the platform.

Verify Smart License Operation for Inbox High Availability

You can use all the commands that are given in the section [Verify Smart License Operation, on page 35](#) to verify the licensing status in the High Availability mode.

The following commands reflect Inbox High Availability (HA) licensing information:

- **show cube status**—Displays CUBE license capacity and the high availability mode.

```
cube-1#sh cube status
CUBE-Version : 14.4
SW-Version : 17.6.1a, Platform ASR1006-X
HA-Type : hot-standby-card-to-card
cube-2#sh cube status
CUBE-Version : 14.4
SW-Version : 17.6.1a, Platform ASR1006-X
HA-Type : hot-standby-card-to-card
```

- **show redundancy states**—Displays the redundancy state of the Route Processors.

```
cube-1#sh redundancy states
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit = Primary
Unit ID = 48

Redundancy Mode (Operational) = sso
```

```

Redundancy Mode (Configured) = sso
Redundancy State              = sso
  Maintenance Mode = Disabled
  Manual Swact = enabled
  Communications = Up

  client count = 135
  client_notification_TMR = 30000 milliseconds
    RF debug mask = 0x0
Gateway monitoring interval = 0 secs
cube-1#
cube-2#sh redundancy states
  my state = 8 -STANDBY HOT
  peer state = 13 -ACTIVE
    Mode = Duplex
    Unit = Secondary
    Unit ID = 49

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State              = sso
  Maintenance Mode = Disabled
  Manual Swact = cannot be initiated from this the standby unit
  Communications = Up

  client count = 135
  client_notification_TMR = 30000 milliseconds
    RF debug mask = 0x0
Gateway monitoring interval = 0 secs
cube-2#

```

- **show license summary**—Displays license summary information.

```

cube-1#sh license summary (active)
License Usage:
  License                Entitlement tag                Count Status
  -----
  adventerprise          (ASR_1000_AdvEnterprise)          1 IN USE
  ipbase                  (ASR_1000_Ipbase)                 1 IN USE
  CUBE_Standard_Session  (CUBE_T_STD)                       10 IN USE

cube-1#

cube-2#sh license summary (standby)
License Usage:
  License                Entitlement tag                Count Status
  -----
  adventerprise          (ASR_1000_AdvEnterprise)          1 IN USE
  ipbase                  (ASR_1000_Ipbase)                 1 IN USE
cube-2#

```

Syslog Messages

- In B2BHA mode, syslog messages are generated by the active CUBE router and not the standby router. The following is a syslog output for an active CUBE router in B2BHA mode:

```
%CUBE-5-LICENSE_INFO: Requesting for 3 CUBE Enhanced trunk licenses
```



CHAPTER 6

Configure Dial Peers

- [Overview, on page 45](#)
- [Preferences, on page 47](#)
- [Configure Inbound and Outbound Dial-Peer Matching, on page 48](#)

Overview

Cisco Unified Border Element (CUBE) allows VoIP-to-VoIP connection by routing calls from one VoIP dial peer to another. VoIP interworking is achieved by connecting an inbound dial peer with an outbound dial peer.



Note All CUBE Enterprise deployments must have signaling and media bind statements that are specified at the dial-peer or Voice Class Tenants level. For voice call tenants, you must apply tenants to dial-peers used for CUBE call flows if these dial-peers do not have bind statements that are specified.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

A dial peer is a static routing table, mapping phone numbers to interfaces or IP addresses.

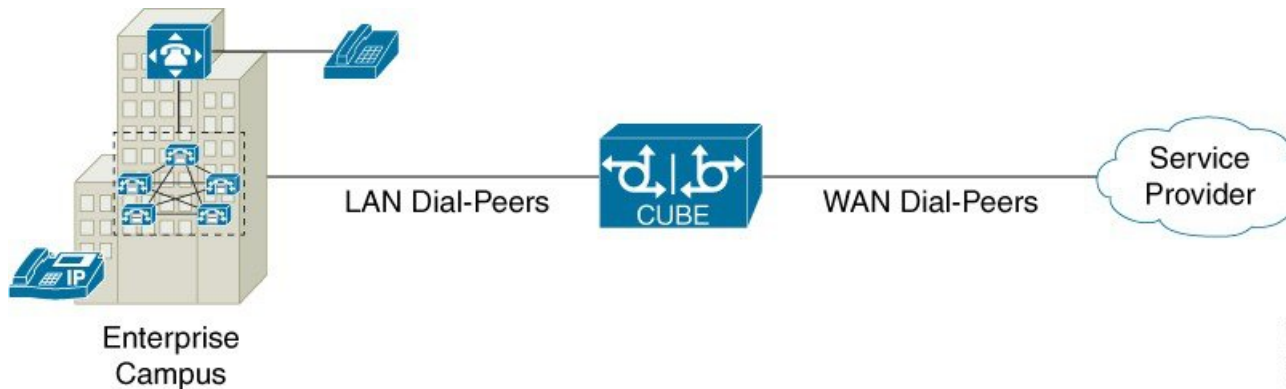
A call leg is a logical connection between two routers or between a router and a VoIP endpoint. A dial peer is associated or matched to each call leg according to attributes that define a packet-switched network, such as the destination address.

Voice-network dial peers are matched to call legs based on configured parameters, after which an outbound dial peer is provisioned to an external component using the component's IP address. For more information, refer to the [Dial Peer Configuration Guide](#).

Dial-peer matching is done based on the VRF ID associated with a particular interface. For more information, see [Inbound Dial-Peer Matching Based on Multi-VRF, on page 718](#).

In CUBE, dial peers are classified as LAN dial peers and WAN dial peers based on the connecting entity from which CUBE sends or receives calls.

Figure 7: LAN and WAN Dial Peers



A dial peer is used to send or receive calls between CUBE and the PBX (PBX)—a system of phone extensions within enterprise. Following are examples of inbound and outbound dial peers:

Figure 8: Dial Peers

Inbound Dial-Peer for calls from CUCM to CUBE

```
dial-peer voice 100 voip
description *** Inbound LAN side dial-peer ***
incoming called-number 9T
session protocol sipv2
codec g711ulaw
dtmf-relay rtp-nte
```

CUCM sending 9
+ All digits dialed
(Outgoing calls)

Incoming call number
used to match the
inbound LAN dial peer

Outbound Dial-Peer for calls from CUBE to CUCM

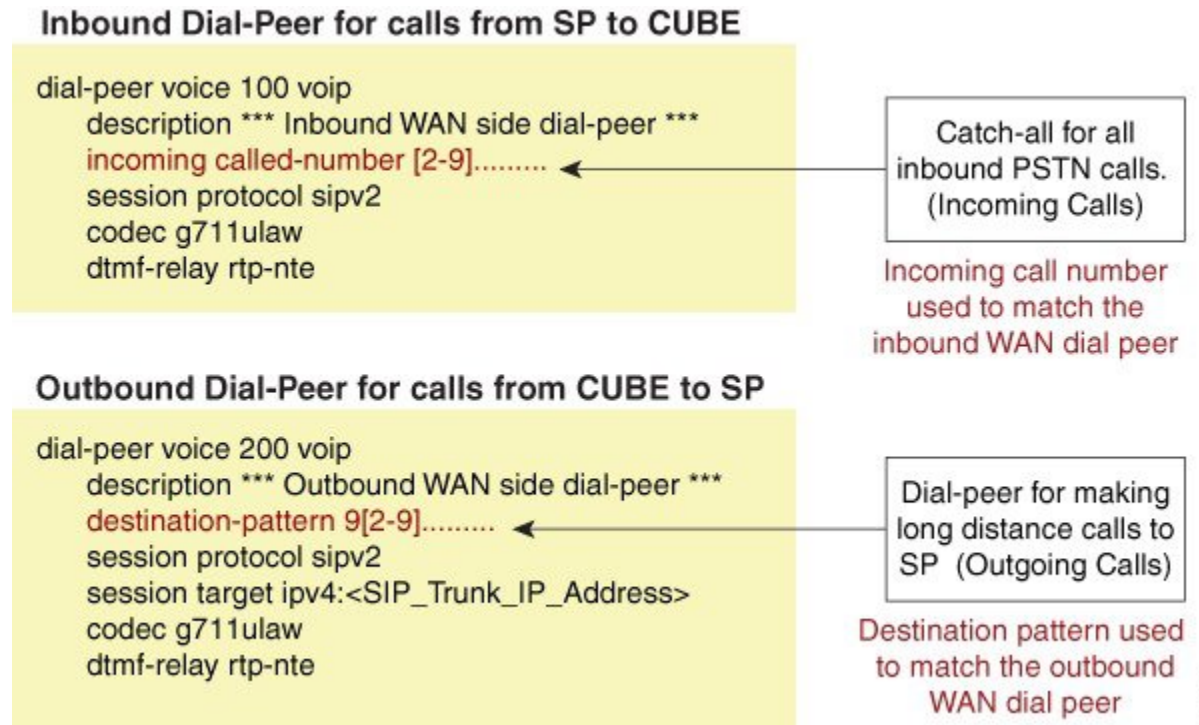
```
dial-peer voice 200 voip
description *** Outbound LAN side dial-peer ***
destination-pattern [2-9].....
session protocol sipv2
session target ipv4:<CUCM_Address>
codec g711ulaw
dtmf-relay rtp-nte
```

SP will be sending
10 digits inbound
(Incoming Calls)

Destination pattern
used to match the
outbound LAN dial peer

Another set of dial peer is used to send or receive calls between CUBE and the SIP trunk provider. Given below are examples of inbound and outbound dial peers.

Figure 9: Other Set of dial peers



371526

Preferences

The following is the order in which inbound dial-peer is matched for SIP call-legs:

- **voice class uri** *URI-class-identifier* with **incoming uri** {*via*} *URI-class-identifier*
- **voice class uri** *URI-class-identifier* with **incoming uri** {*request*} *URI-class-identifier*
- **voice class uri** *URI-class-identifier* with **incoming uri** {*to*} *URI-class-identifier*
- **voice class uri** *URI-class-identifier* with **incoming uri** {*from*} *URI-class-identifier*
- **incoming called-number** *DNIS-string*
- **answer-address** *ANI-string*

The following is the order in which outbound dial-peer is matched for SIP call-legs:

- **destination route-string**
- **destination** *URI-class-identifier* with **target carrier-id** *string*
- **destination-pattern** with **target carrier-id** *string*
- **destination** *URI-class-identifier*
- **destination-pattern**
- **target carrier-id** *string*



Note CUCME System dial peers take preference over configured SIP Dial peers.

Configure Inbound and Outbound Dial-Peer Matching

The following commands are used for inbound and outbound dial peer matching:

Table 5: Incoming Dial-Peer Matching

Command in Dial-Peer Configuration	Description	Call Setup Element
incoming called-number <i>DNIS-string</i>	This command uses the destination number that was called to match the incoming call leg to an inbound dial peer. This number is called the Dialed Number Identification Service (DNIS) number.	DNIS number
answer-address <i>ANI-string</i>	This command uses the calling number to match the incoming call leg to an inbound dial peer. This number is called the originating calling number or Automatic Number Identification (ANI) string.	ANI string
destination-pattern <i>ANI-string</i>	This command uses the inbound call leg to the inbound dial peer.	ANI string for inbound
{incoming called incoming calling} e164-pattern-map <i>pattern-map-group-id</i>	This command uses a group of incoming called (DNIS) or incoming calling (ANI) number patterns to match the inbound call leg to an inbound dial peer. The command calls a globally defined voice class identifier where the E.164 pattern groups are configured.	E.164 Patterns
voice class uri <i>URI-class-identifier</i> with incoming uri {from request to via} URI-class-identifier	This command uses the directory URI (Uniform Resource Identifier) number of an incoming INVITE from a SIP entity to match an inbound dial peer. This directory URI is part of the SIP address of a device. The command calls a globally defined voice class identifier where the directory URI is configured.	Directory URI

Table 6: Outgoing Dial-Peer Matching

Dial-Peer Command	Description	Call Setup Element
destination-pattern <i>DNIS-string</i>	This command uses DNIS string to match the outbound call leg to the outbound dial peer.	DNIS string for outbound ANI string for inbound

Dial-Peer Command	Description	Call Setup Element
destination <i>URI-class-identifier</i>	<p>This command uses the directory URI (Uniform Resource Identifier) number to match the outgoing call leg to an outgoing dial peer. This directory URI is part of the SIP address of a device.</p> <p>The command actually refers to a globally defined voice class identifier where the directory URI is configured.</p>	Directory URI
destination e164-pattern-map <i>pattern-map-group-id</i>	<p>This command uses a group of destination number patterns to match the outbound call leg to an outbound dial peer.</p> <p>The command calls a globally defined voice class identifier where the E.164 pattern groups are configured.</p>	E.164 patterns



CHAPTER 7

DTMF Relay

- [Overview, on page 51](#)
- [Interoperability and Priority with Multiple DTMF Relay Methods, on page 55](#)
- [Configure DTMF Relay, on page 58](#)
- [Verify DTMF Relay, on page 58](#)

Overview

The DTMF Relay feature allows Cisco Unified Border Element (CUBE) to send dual-tone multifrequency (DTMF) digits over IP.

This chapter talks about DTMF tones, DTMF relay mechanisms, how to configure DTMF relays, and interoperability and priority with multiple relay methods.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 7: Feature Information for DTMF Relay

Feature Name	Releases	Feature Information
Support for sip-info to rtp-nte DTMF relay mechanism for SIP-SIP calls	Cisco IOS XE Everest 16.6.1	This feature adds support for sip-info to rtp-nte DTMF relay mechanism for SIP-SIP calls.

DTMF Tones

DTMF tones are used during a call to signal to a far-end device; these signals are for navigating a menu system, entering data, or for other types of manipulation. They are processed differently from the DTMF tones that are sent during the call setup as part of the call control. TDM interfaces on Cisco devices support DTMF by default. Cisco VoIP dial-peers do not support DTMF relay by default and require DTMF relay capabilities to be enabled.



Note DTMF tones sent by phones do not traverse the CUBE.

DTMF Relay

Dual-Tone Multifrequency (DTMF) relay is the mechanism for sending DTMF digits over IP. The VoIP dial peer can pass the DTMF digits either in a band or out of band.

In-band DTMF-Relay passes the DTMF digits using the RTP media stream and uses a special payload type identifier in the RTP header to distinguish DTMF digits from voice communication. This method is more likely to work on lossless codecs, such as G.711.

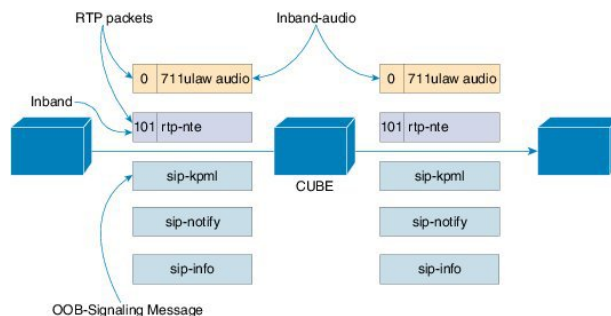


Note The main advantage of DTMF relay is that low-bandwidth codecs like G.729 and G.723 is sent with greater fidelity when sent using in-band DTMF relay. Without the use of DTMF relay, calls established with low-bandwidth codecs may have trouble accessing automated DTMF-based systems, such as voicemail, menu-based Automatic Call Distributor (ACD) systems, and automated banking systems.

Out-of-band DTMF-Relay passes DTMF digits using a signaling protocol (SIP) instead of using the RTP media stream.

DTMF relay prevents loss of integrity of DTMF digits that are caused by VoIP compressed codecs. The relayed DTMF is then regenerated transparently on the peer side.

Figure 10: DTMF Relay Mechanism



DTMF relay mechanisms that are supported on VoIP dial-peers are listed below based on the keywords used to configure them. The DTMF relay mechanism can be either out-of-band (SIP) or in-band (RTP).

- **sip-notify**—This method is available on SIP dial peers only. This is a Cisco proprietary out-of-band DTMF relay mechanism that transports DTMF signals using SIP-Notify message. The SIP Call-Info

header indicates the use of the SIP-Notify DTMF relay mechanism. The message is acknowledged with a 18x or 200 response message containing a similar SIP Call-Info header.

The Call-Info header for a NOTIFY-based out-of-band relay is as follows:

```
Call-Info: <sip: address>; method="NOTIFY;Event=telephone-event;Duration=msec"
```

DTMF relay digits are sent as 4 bytes in a binary encoded format.

This mechanism is useful for communicating with SCCP IP phones that do not support in-band DTMF digits and analog phones that are attached to analog voice ports (FXS) on the router.

If multiple DTMF relay mechanisms are enabled on a SIP dial peer and are negotiated successfully, NOTIFY-based out-of-band DTMF relay takes precedence.

- **sip-kpml**— This is an out-of-band DTMF relay mechanism that is defined by RFC 4730 that registers the DTMF signals using SIP-Subscribe messages and transports the DTMF signals using SIP-Notify messages containing an XML-encoded body. This method is also known as Key Press Markup Language.

If you configure KPML on the dial peer, the gateway sends INVITE messages with KPML in the Allow-Events header.

The use of this method is to register SIP endpoints to Cisco Unified Communications Manager(CUCM) or Cisco Unified Communications Manager Express(CME). This method is useful for nonconferencing calls and for interoperability between SIP products and SIP phones.

If you configure rtp-nte, sip-notify, and sip-kpml, the outgoing INVITE contains an SDP with rtp-nte payload, a SIP Call-Info header, and an Allow-Events header with KPML.

The following SIP-Notify message is a sample that is taken after the subscription has taken place. The endpoints transmit digits using SIP-Notify messages with KPML events through XML. In the following example, the digit "1" is being transmitted:

```
NOTIFY sip:192.168.105.25:5060 SIP/2.0
Event: kpml
<?xml version="1.0" encoding="UTF-8"?>
<kpml-response version="1.0" code="200" text="OK" digits="1" tag="dtmf"/>
```

- **sip-info**—The sip-info method is available only on SIP dial peers. This is an out-of-band DTMF relay mechanism that registers the DTMF signals using SIP-Info messages. The body of the SIP message consists of signaling information and uses the Content-Type application/dtmf-relay.

The method is always enabled for SIP dial peers, and is invoked when a SIP INFO message is received with DTMF relay content.

This following sample message shows that a SIP INFO message received with specifics about the DTMF tone to be generated. The combination of the From, To, and Call-ID headers identifies the call leg. The signal and duration headers specify the digit, in this case 1, and duration, 160 milliseconds in the example, for DTMF tone play.

```
INFO sip:2143302100@172.17.2.33 SIP/2.0
Via: SIP/2.0/UDP 172.80.2.100:5060
From: <sip:9724401003@172.80.2.100>;tag=43
To: <sip:2143302100@172.17.2.33>;tag=9753.0207
Call-ID: 984072_15401962@172.80.2.100
CSeq: 25634 INFO
Supported: 100rel
Supported: timer
Content-Length: 26
Content-Type: application/dtmf-relay
Signal= 1
Duration= 160
```

- **rtp-nte**—Real-Time Transport Protocol (RTP) Named phone Events (NTE). This is an in-band DTMF relay mechanism that is defined by RFC2833. RFC2833 defines formats of NTE-RTP packets that are used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints. DTMF tones are sent as packet data after call media has been established using the RTP stream and are distinguished from the audio by the RTP payload type field, preventing compression of DTMF-based RTP packets. For example, the audio of a call is sent on a session with an RTP payload type that identifies it as G.711 data, and the DTMF packets are sent with an RTP payload type that identifies them as NTEs. The consumer of the stream utilizes the G.711 packets and the NTE packets separately.

The SIP NTE DTMF relay feature provides reliable digit relay.



Note Payload type 96 and 97 is used for fax by default in Cisco devices. A third-party device may use payload type 96 and 97 for DTMF. In such scenarios, we recommend you to perform one of the following:

- Change the payload type for fax in both incoming and outgoing dial-peers using **rtp payload-type** command
- Use **assymmetric payload dtmf** command

For more information on configuring rtp payload-type and asymmetric payload DTMF, see [Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls](#).

Payload types and attributes of this method are negotiated between the two ends at call setup using the Session Description Protocol (SDP) within the body section of the SIP message.



Note This method should not be confused with the “Voice in-band audio/G711” transport because the latter is just the audible tones is passed as normal audio without any relay signaling method being “aware” or involved in the process. This is plain audio passing through end-to-end using the G711Ulaw/Alaw codec.

- **cisco-rtp**—This is an in-band DTMF relay mechanism that is Cisco proprietary, where the DTMF digits are encoded differently from the audio and are identified as a payload type 121. The DTMF digits are part of the RTP data stream and distinguished from the audio by the RTP payload type field. This method is not supported by CUCM and its use has been discontinued.
- **G711 audio**—This is an in-band DTMF relay mechanism that is enabled by default and requires no configuration. Digits are transmitted within the audio of the phone conversation, that is, it is audible to the conversation partners; therefore, only uncompressed codecs like g711 alaw or ulaw can carry in-band DTMF reliably. Female voices are known to, sometimes, trigger the recognition of a DTMF tone.

Digits are passed along just like the rest of your voice as normal audio tones with no special coding or markers using the same codec as your voice does and are generated by your phone.

Interoperability and Priority with Multiple DTMF Relay Methods

- CUBE negotiates both **rtp-nte** and **sip-kpml** if both are supported and advertised in the incoming INVITE. However, CUBE relies on the **rtp-nte** DTMF method to receive digits and a SUBSCRIBE if **sip-kpml** is not initiated. CUBE still accepts SUBSCRIBEs for KPML. This prevents double-digit reporting problems at CUBE.
- CUBE negotiates to one of the following:
 - **cisco-rtp**
 - **rtp-nte**
 - **rtp-nte** and **kpml**
 - **kpml**
 - **sip-notify**
- If you configure **rtp-nte**, **sip-notify**, and **sip-kpml**, the outgoing INVITE contains a SIP Call-Info header, an Allow-Events header with KPML, and an sdp with **rtp-nte** payload.
- If you configure more than one out-of-band DTMF method, preference goes from highest to lowest in the order of configuration.
- CUBE selects DTMF relay mechanisms using the following priority:
 - **sip-notify** or **sip-kpml**
(highest priority)
 - **rtp-nte**
 - **None**—Send DTMF in-band

DTMF Interoperability Table

This table provides the DTMF interoperability information between various DTMF relay types in different call flow scenarios. For instance, if you need to configure **sip-kpml** on an inbound dial peer and **RTP-NTE** on an outbound dial peer in an RTP-RTP Flow through configuration, refer table 3 to see that the combination is supported. The call scenarios provided are as follows:

- RTP-RTP Flow-Through
- RTP-RTP with transcoder Flow-Through
- RTP-RTP Flow Around
- SRTP-RTP Flow Through

Table 8: RTP-RTP Flow-Through

	outbound dial-peer protocol	SIP				Inband
inbound dial-peer protocol	DTMF Relay Type	rtp-nte	sip-kpml	sip-notify	sip-info	Voice Inband (G.711)
SIP	rtp-nte	Supported	Supported	Supported		Supported*
	sip-kpml	Supported	Supported			
	sip-notify	Supported		Supported		
	sip-info	Supported 1				
Inband	Voice Inband (G.711)	Supported*				Supported

¹ Supported from Cisco IOS XE Everest 16.6.1 onwards for calls that do not involve DSP resources.

* Media resource is required (Transcoder) for Cisco IOS and IOS XE versions.

Table 9: RTP-RTP with DSP involved Flow-Through Calls

	outbound dial-peer protocol	SIP				Inband
inbound dial-peer protocol	DTMF Relay Type	rtp-nte	sip-kpml	sip-notify	sip-info	Voice Inband (G.711)
SIP	rtp-nte	Supported				Supported
	sip-kpml		Supported			
	sip-notify			Supported		
	sip-info					
Inband	Voice Inband (G.711)	Supported				

Table 10: RTP-RTP Flow Around

	outbound dial-peer protocol	SIP				Inband
inbound dial-peer protocol	DTMF Relay Type	rtp-nte	sip-kpml	sip-notify	sip-info	Voice Inband (G.711)
SIP	rtp-nte	Supported				Supported*
	sip-kpml		Supported			
	sip-notify			Supported		
	sip-info					
Inband	Voice Inband (G.711)	Supported*				Supported

* Media resource is required (Transcoder) for Cisco IOS and IOS XE versions. CUBE falls back to flow-through mode if media resource is unavailable.

Table 11: SRTP-RTP Flow Through

	outbound dial-peer protocol	SIP				Inband
inbound dial-peer protocol	DTMF Relay Type	rtp-nte	sip-kpml	sip-notify	sip-info	Voice Inband (G.711)
SIP	rtp-nte	Supported	Supported	Supported		Supported
	sip-kpml	Supported	Supported			
	sip-notify	Supported		Supported		
	sip-info					
Inband	Voice Inband (G.711)	Supported				Supported



Note For calls sent from an in-band (RTP-NTE) to an out-of band method, configure the **dtmf-relay rtp-nte digit-drop** command on the inbound dial-peer and the desired out-of-band method on the outgoing dial-peer. Otherwise, the same digit is sent in OOB as well as in-band, and gets interpreted as duplicate digits by the receiving end. When the digit-drop option is configured on the inbound leg, CUBE suppresses NTE packets and only relay digits using the OOB method configured on the outbound leg.

Configure DTMF Relay

You can configure DTMF relay using the `dtmf-relay method1 [...[method6]]` command in the VoIP dial peer. DTMF negotiation is performed based on the matching inbound dial-peer configuration.

The `method` variable used here can be any of the following:

- `sip-notify`
- `sip-kpml`
- `sip-info`
- `rtp-nte [digit-drop]`
- `ciso-rtp`

Multiple DTMF methods may be configured on CUBE simultaneously in order to minimize MTP requirements. If you configure more than one out-of-band DTMF method, preference goes from highest to lowest in the order of configuration. If an endpoint does not support any of the DTMF relay mechanism configured on CUBE, an MTP or transcoder is required.

The following table lists the DTMF relay types supported.

Table 12: Supported DTMF Relay Methods

In-band	<code>rtp-nte</code>
Out-of-band	<code>sip-notify, sip-kpml, sip-info</code>

Verify DTMF Relay

SUMMARY STEPS

1. `show sip-ua calls`
2. `show sip-ua calls dtmf-relay sip-info`
3. `show sip-ua history dtmf-relay kpml`
4. `show sip-ua history dtmf-relay sip-notify`

DETAILED STEPS

Step 1 `show sip-ua calls`

The following sample output shows that the DTMF method is SIP-KPML.

Example:

```
Device# show sip-ua calls
SIP UAC CALL INFO
Call 1
```

```

SIP Call ID           : 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
  State of the call    : STATE_ACTIVE (7)
  Substate of the call : SUBSTATE_NONE (0)
  Calling Number       :
  Called Number        : 8888
  Bit Flags            : 0xD44018 0x100 0x0
  CC Call ID          : 6
  Source IP Address (Sig) : 192.0.2.1
  Destn SIP Req Addr:Port : 192.0.2.2:5060
  Destn SIP Resp Addr:Port : 192.0.2.3:5060
  Destination Name     : 192.0.2.4.250
  Number of Media Streams : 1
  Number of Active Streams: 1
  RTP Fork Object      : 0x0
  Media Mode           : flow-through
  Media Stream 1
    State of the stream : STREAM_ACTIVE
    Stream Call ID      : 6
    Stream Type         : voice-only (0)
    Negotiated Codec    : g711ulaw (160 bytes)
  Codec Payload Type   : 0
    Negotiated Dtmf-relay : sip-kpml
    Dtmf-relay Payload Type : 0
    Media Source IP Addr:Port : 192.0.2.5:17576
    Media Dest IP Addr:Port  : 192.0.2.6:17468
    Orig Media Dest IP Addr:Port : 0.0.0.0:0
  Number of SIP User Agent Client(UAC) calls: 1
SIP UAS CALL INFO
  Number of SIP User Agent Server(UAS) calls: 0

```

Step 2 show sip-ua calls dtmf-relay sip-info

The following sample output displays active SIP calls with INFO DTMF Relay mode.

Example:

```

Device# show sip-ua calls dtmf-relay sip-info

Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID           : 9598A547-5C1311E2-8008F709-2470C996@172.27.161.122
  State of the call    : STATE_ACTIVE (7)
  Calling Number       : sipp
  Called Number        : 3269011111
  CC Call ID          : 2
No.      Timestamp           Digit           Duration
=====
0      01/12/2013 17:23:25.615  2                250
1      01/12/2013 17:23:25.967  5                300
2      01/12/2013 17:23:26.367  6                300

Call 2
SIP Call ID           : 1-29452@172.25.208.177
  State of the call    : STATE_ACTIVE (7)
  Calling Number       : sipp
  Called Number        : 3269011111
  CC Call ID          : 1
No.      Timestamp           Digit           Duration
=====
0      01/12/2013 17:23:25.615  2                250
1      01/12/2013 17:23:25.967  5                300
2      01/12/2013 17:23:26.367  6                300

```

Number of SIP User Agent Client(UAC) calls: 2

SIP UAS CALL INFO

Call 1

SIP Call ID : 1-29452@172.25.208.177
 State of the call : STATE_ACTIVE (7)
 Calling Number : sipp
 Called Number : 3269011111
 CC Call ID : 1

No.	Timestamp	Digit	Duration
0	01/12/2013 17:23:25.615	2	250
1	01/12/2013 17:23:25.967	5	300
2	01/12/2013 17:23:26.367	6	300

Call 2

SIP Call ID : 9598A547-5C1311E2-8008F709-2470C996@172.27.161.122
 State of the call : STATE_ACTIVE (7)
 Calling Number : sipp
 Called Number : 3269011111
 CC Call ID : 2

No.	Timestamp	Digit	Duration
0	01/12/2013 17:23:25.615	2	250
1	01/12/2013 17:23:25.967	5	300
2	01/12/2013 17:23:26.367	6	300

Number of SIP User Agent Server(UAS) calls: 2

Step 3 show sip-ua history dtmf-relay kpml

The following sample output displays SIP call history with KMPL DTMF Relay mode.

Example:

Device# show sip-ua history dtmf-relay kpml

Total SIP call legs:2, User Agent Client:1, User Agent Server:1

SIP UAC CALL INFO

Call 1

SIP Call ID : D0498774-F01311E3-82A0DE9F-78C438FF@10.86.176.119
 State of the call : STATE_ACTIVE (7)
 Calling Number : 2017
 Called Number : 1011
 CC Call ID : 257

No.	Timestamp	Digit	Duration
-----	-----------	-------	----------

Call 2

SIP Call ID : 22BC36A5-F01411E3-81808A6A-5FE95113@10.86.176.142
 State of the call : STATE_ACTIVE (7)
 Calling Number : 2017
 Called Number : 1011
 CC Call ID : 256

No.	Timestamp	Digit	Duration
-----	-----------	-------	----------

Number of SIP User Agent Client(UAC) calls: 2

SIP UAS CALL INFO

Call 1

SIP Call ID : 22BC36A5-F01411E3-81808A6A-5FE95113@10.86.176.142
 State of the call : STATE_ACTIVE (7)
 Calling Number : 2017

```

    Called Number      : 1011
    CC Call ID        : 256
No.      Timestamp      Digit      Duration
=====
Call 2
SIP Call ID          : D0498774-F01311E3-82A0DE9F-78C438FF@10.86.176.119
  State of the call   : STATE_ACTIVE (7)
  Calling Number      : 2017
  Called Number       : 1011
  CC Call ID         : 257
No.      Timestamp      Digit      Duration
=====

    Number of SIP User Agent Server(UAS) calls: 2

```

Step 4 show sip-ua history dtmf-relay sip-notify

The following sample output displays SIP call history with SIP Notify DTMF Relay mode.

Example:

```

Device# show sip-ua history dtmf-relay sip-notify

Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID          : 29BB98C-F01311E3-8297DE9F-78C438FF@10.86.176.119
  State of the call   : STATE_ACTIVE (7)
  Calling Number      : 2017
  Called Number       : 1011
  CC Call ID         : 252
No.      Timestamp      Digit      Duration
=====
Call 2
SIP Call ID          : 550E973B-F01311E3-817A8A6A-5FE95113@10.86.176.142
  State of the call   : STATE_ACTIVE (7)
  Calling Number      : 2017
  Called Number       : 1011
  CC Call ID         : 251
No.      Timestamp      Digit      Duration
=====

    Number of SIP User Agent Client(UAC) calls: 2

SIP UAS CALL INFO
Call 1
SIP Call ID          : 550E973B-F01311E3-817A8A6A-5FE95113@10.86.176.142
  State of the call   : STATE_ACTIVE (7)
  Calling Number      : 2017
  Called Number       : 1011
  CC Call ID         : 251
No.      Timestamp      Digit      Duration
=====
Call 2
SIP Call ID          : 29BB98C-F01311E3-8297DE9F-78C438FF@10.86.176.119
  State of the call   : STATE_ACTIVE (7)
  Calling Number      : 2017
  Called Number       : 1011
  CC Call ID         : 252
No.      Timestamp      Digit      Duration
=====

```

Number of SIP User Agent Server (UAS) calls: 2



CHAPTER 8

Introduction to Codecs

- [Overview, on page 63](#)
- [Restrictions, on page 64](#)
- [Media Transmission, on page 65](#)
- [Voice Activity Detection, on page 65](#)
- [VoIP Bandwidth Requirements, on page 66](#)
- [Supported Audio and Video Codecs, on page 68](#)
- [Configure Codecs, on page 69](#)
- [Configuration Examples for Codecs, on page 73](#)

Overview

A codec is a device or software capable of encoding or decoding a digital data stream or signal. Audio codecs can encode or decode a digital data stream of audio. Video codecs encode or decode digital video streams.

This chapter describes the basics of encoding digital voice samples using codecs and how to configure them.

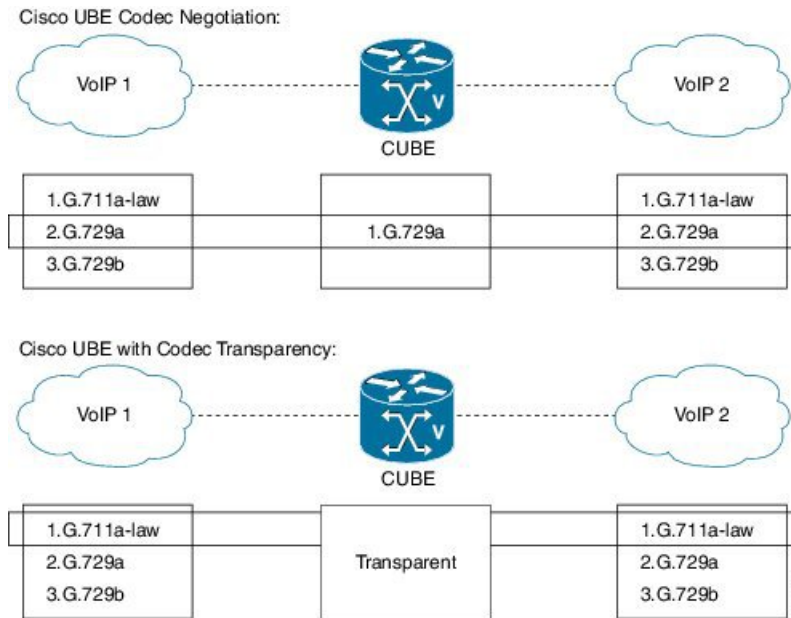
Cisco Unified Border Element (CUBE) uses codecs to compress digital voice samples to reduce bandwidth usage per call.

Configuring codecs allows the CUBE to act as a demarcation point on a VoIP network and allows calls on a specific dial peer to be established only if the desired codec criteria are satisfied. Also, preferences can be used to determine which codecs are selected over others.

If codec filtering is not required, CUBE also supports transparent codec negotiations. The codec filtering enables negotiations between endpoints with CUBE leaving the codec information untouched.

The following illustrations show how codec negotiation is performed on CUBE. Two VoIP clouds must be interconnected. In this scenario, both VoIP 1 and VoIP 2 networks have G.711 a-law that is configured as the preferred codec.

Figure 11: Codec Negotiation on CUBE



In the first example, the CUBE router is configured to use the G.729a codec. This can be done by using the appropriate codec command on both VoIP dial peers. When a call is set up, CUBE accepts only G.729a calls, thus influencing the codec negotiation.

In the second example, the CUBE dial peers are configured with a transparent codec and this leaves the codec information that is contained within the call signaling untouched. Because both VoIP 1 and VoIP 2 have G.711 a-law as their first choice, the resulting call is a G.711 a-law call.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Restrictions

While using the voice-class codec transparent, only the offer is passed transparently (without filtering). Codec filtering is carried out on SDP content in ANSWER messages. Only the first codec in the offer list is included in the outbound message.



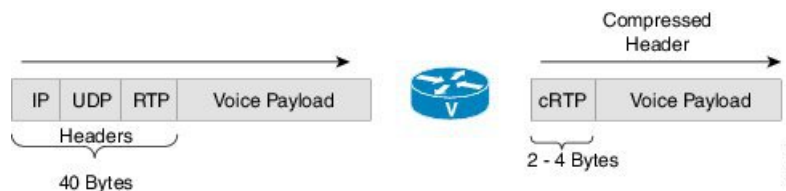
Note You can use 'pass-thru content sdp,' if you do not want to involve CUBE in the codec negotiation.

Media Transmission

When a VoIP call is established, the digitized audio and video samples must be transmitted. These samples are often called the media payload. The following media protocols specify the standards related to transmission of media payload in VoIP networks:

- Real-Time Transport Protocol (RTP)—RTP is a Layer 4 protocol that is encapsulated inside UDP segments. RTP carries the actual media voice samples in a call.
- Real-Time Control Protocol (RTCP)—RTCP is a companion protocol to RTP. Both RTP and RTCP operate at Layer 4 and are encapsulated in UDP. RTP and RTCP typically use UDP ports 16384 to 32767, though these ranges may vary according to hardware platform. RTP uses the even port numbers in that range, whereas RTCP uses the odd port numbers. While RTP is responsible for carrying the media payload, RTCP carries information about the RTP stream such as latency, jitter, packets, and octets sent and received.
- Compressed RTP (CRTP)—One of the challenges with RTP is its overhead. Specifically, the combined IP, UDP, and RTP headers are approximately 40 bytes in size, whereas a common voice payload size on a VoIP network is only 20 bytes, which includes 20 ms of voice by default. In that case, the header is twice the size of the payload. cRTP is used for RTP header compression and can reduce the 40-byte header to 2 or 4 bytes in size (depending on whether UDP checksums are in use), as shown in the figure below.

Figure 12: Compressed RTP



- Secure RTP (SRTP)—To help prevent an attacker from intercepting and decoding or possibly manipulating media packets, SRTP encrypts RTP packets. In addition, SRTP provides message authentication, integrity checking, and protection against replay attacks.

VPN technology is used to protect traffic between sites. Sending SRTP via a VPN tunnel results in the encryption of traffic that is already secure, adding significant overhead and bandwidth needs. It is recommended that SRTP is used for media traffic, and that is excluded from VPN tunnels. By encrypting media directly on communicating endpoints, it is possible to realise a more secure solution, that requires less bandwidth and infrastructure investment.

Voice Activity Detection

Voice Activity Detection (VAD) is a technology that works with the human nature of voice conversations, mainly that one person listens while the other talks. VAD classifies traffic as speech, unknown, and silence. Speech and unknown payloads are transported, but silence is dropped. This accounts for approximately 30 percent savings in bandwidth over time.

VAD can significantly reduce the amount of bandwidth that is required by a media stream. However, VAD has a few negative attributes that must be considered. Because no packets are sent during silence, the listener

can get the impression that the talker has been disconnected. Another characteristic is that it takes a moment for VAD to recognize the speech as having started again, and as a result, the first part of the sentence can be clipped. This can be annoying to the listening party. Music on Hold (MoH) and fax can also cause VAD to become ineffective because the media stream is constant.

VAD is enabled by default in CUBE dial peers as long as the codec selected supports it. VAD can be disabled at the VoIP dial peer using the **no vad** command. Some codecs, such as G.729b and G.729ab, support Comfort Noise Generation (CNG). When VAD is enabled, white noise is played to the listener during times when no packets are received. This leads the listener to believe that call is still connected. Cisco IP Phones and most gateways support CNG.

G.729 Annex-B and G.723.1 Annex-A include an integrated VAD function, but otherwise performs the same as G.729 and G.723.1, respectively.



Note VAD to NO-VAD calls is not supported by Cisco Unified Border Element (CUBE). This confirms that CUBE cannot generate comfort noise to fill periods of silence.

VoIP Bandwidth Requirements

The amount of bandwidth that is required varies by the codec and the transmission media. Two events require bandwidth. The media stream itself requires bandwidth between 17–106 kbps depending on codec, header compression, and Layer 2 and 3 headers. In addition, call signaling must be taken into account. While bandwidth required by call signaling is much smaller, problems occur when this traffic is dropped in congested networks.

Table 13: Protocol Header Size Assumptions

Protocol	Header size
IP	20 bytes
UDP	8 bytes
RTP	12 bytes
cRTP	Reduces size of IP, UDP, RTP to 2 or 4 bytes

The table below gives calculations for the default voice payload sizes in Cisco Unified Communications Manager or CUBE. For additional calculations, including different voice payload sizes and other protocols, use the [TAC Voice Bandwidth Codec Calculator](#) (registered customers only). For an explanation of each of the column headings, see the table below.

Table 14: Codec and Bandwidth Information

Codec & Bit Rate (kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Payload Size (ms) Packets Per Second (PPS)	Bandwidth Ethernet (kbps)
G.711 (64 kbps)	80	10	4.1	160	20	50	87.2
G.729 (8 kbps)	10	10	3.92	20	20	50	31.2

Codec & Bit Rate (kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Payload Size (ms) Packets Per Second (PPS)	Bandwidth Ethernet (kbps)
G.723.1 (6.3 kbps)	24	30	3.9	24	30	33.3	21.9
G.723.1 (5.3 kbps)	20	30	3.8	20	30	33.3	20.8
G.726 (32 kbps)	20	5	3.85	80	20	50	55.2
G.726 (24 kbps)	15	5		60	20	50	47.2
G.728 (16 kbps)	10	5	3.61	60	30	33.3	31.5
G722_64k(64 kbps)	80	10	4.13	160	20	50	87.2
ilbc_mode_20(15.2 kbps)	38	20	3.95	38	20	50	38.4
ilbc_mode_30(13.33 kbps)	50	30	3.88	50	30	33.3	28.8
OPUS							

Table 15: Explanation of Terms

Codec Bit Rate (kbps)	Based on the codec, this is the number of bits per second that must be transmitted to deliver a voice call. (codec bit rate = codec sample size / codec sample interval).
Codec Sample Size (Bytes)	Size (Bytes) Based on the codec, this is the number of bytes captured by the digital signal processor (DSP) at each codec sample interval. For example, the G.729 coder operates on sample intervals of 10 ms, corresponding to 10 bytes (80 bits) per sample at a bit rate of 8 kbps. (codec bit rate = codec sample size / codec sample interval).
Codec Sample Interval (ms)	This is the sample interval at which the codec operates. For example, the G.729 coder operates on sample intervals of 10 ms, corresponding to 10 bytes (80 bits) per sample at a bit rate of 8 kbps. (codec bit rate = codec sample size / codec sample interval).
MOS	MOS is a system of grading the voice quality of telephone connections. With MOS, a wide range of listeners judge the quality of a voice sample on a scale of one (bad) to five (excellent). The scores are averaged to provide the MOS for the codec.
Voice Payload Size (Bytes)	The voice payload size represents the number of bytes (or bits) that are filled into a packet. The voice payload size must be a multiple of the codec sample size. For example, G.729 packets can use 10, 20, 30, 40, 50, or 60 bytes of voice payload size.

Voice Payload Size (ms)	Payload Size (ms) The voice payload size can also be represented in terms of the codec samples. For example, a G.729 voice payload size of 20 ms (two 10 ms codec samples) represents a voice payload of 20 bytes [(20 bytes * 8) / (20 ms) = 8 kbps]
PPS	PPS represents the number of packets that need to be transmitted every second in order to deliver the codec bit rate. For example, for a G.729 call with voice payload size per packet of 20 bytes (160 bits), 50 packets must be transmitted every second [50 pps = (8 kbps) / (160 bits per packet)]

Supported Audio and Video Codecs

CUBE is required to support the codec used between endpoints. g729r8 is supported by default. All other codecs have to be configured. The following codecs are supported:

Table 16: Audio Codecs Supported on CUBE

Codec Keyword	Codec
aacld	AACLD 90000 bps
clear-channel	Clear Channel 64000 bps (No voice capabilities: data transport only)
g711alaw	G.711 A Law 64000 bps
g711ulaw	G.711 u Law 64000 bps
g722-64	G722-64K 64000 bps
g723ar53	G.723.1 ANNEX-A 5300 bps (contains built-in VAD that cannot be disabled)
g723ar63	G.723.1 ANNEX-A 6300 bps (contains built-in VAD that cannot be disabled)
g723r53	G.723.1 5300 bps
g723r63	G.723.1 6300 bps
g726r16	G.726 16000 bps
g726r24	G.726 24000 bps
g726r32	G.726 32000 bps
g728	G.728 16000 bps
g729br8	G.729 ANNEX-B 8000 bps (contains built-in VAD that cannot be disabled)

Codec Keyword	Codec
g729r8	G.729 8000 bps
gsmamr-nb	GSM AMR-NB 4750 to 12200 bps (contains built-in VAD that cannot be disabled)
ilbc	iLBC 13330 or 15200 bps
isac	iSAC 10 to 32 kbps (variable bit-rate)
mp4a-latm	MP4A-LATM upto 128 kbps
opus	Opus upto 510 kbps
transparent	Transparent; uses the endpoint codec

Table 17: Video Codecs Supported on CUBE

Codec Keyword	Codec
h261	Video Codec H261
h263	Video Codec H263
h263+	Video Codec H263+
h264	Video Codec H264
mpeg4	Video Codec MPEG-4 ISO/IES 14496-2

Configure Codecs

Configure Voice Class Codec and Preference Lists

Preferences determine which codecs are selected over others.

A codec voice class is a construct within which a codec preference order is defined. A codec voice class can then be applied to a dial peer, which then follows its preference order.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class codec tag**
4. Add the following for each audio codec you want to configure in the voice class:
 - **codec preference value codec-type**[**profile profile-tag**]
 - **codec preference value codec-type**[**bytes payload-size fixed-bytes**]

- **codec preference value isac** [mode {adaptive | independent} [bit-rate value framesize { 30 | 60 } [fixed]]]
 - **codec preference value ilbc** [mode frame-size [bytes payload-size]]
 - **codec preference value mp4-latm** [profile tag]
5. Add the following to configure a video codec:
 - **video codec codec**
 6. **exit**
 7. **dial-peer voice number voip**
 8. **voice-class codec tag offer-all**
 9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device> configure terminal	Enters global configuration mode.
Step 3	voice class codec tag Example: Device(config)# voice class codec 10	Enters voice-class configuration mode for the specified codec voice class.
Step 4	Add the following for each audio codec you want to configure in the voice class: <ul style="list-style-type: none"> • codec preference value codec-type[profile profile-tag] • codec preference value codec-type[bytes payload-size fixed-bytes] • codec preference value isac [mode {adaptive independent} [bit-rate value framesize { 30 60 } [fixed]]] • codec preference value ilbc [mode frame-size [bytes payload-size]] • codec preference value mp4-latm [profile tag] 	Configure a codec within the voice class and specify a preference for the codec. This becomes part of a preference list.
Step 5	Add the following to configure a video codec: <ul style="list-style-type: none"> • video codec codec Example: video codec h261	Configures a video codec within the voice class.
Step 6	exit	Exits the current mode.

	Command or Action	Purpose
	Example: Device(config-class)# exit	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 7	dial-peer voice <i>number</i> voip Example: Device(config)# dial-peer voice 1 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 8	voice-class codec <i>tag</i> offer-all Example: Device(config-dial-peer)# voice-class codec 10	Applies the previously configured voice class and associated codecs to a dial peer. <ul style="list-style-type: none"> • The offer-all keyword allows the device to offer all codecs configured in a codec voice class.
Step 9	end Example: Device(config-dial-peer)# end	Returns to privileged EXEC mode.

Configure Audio and Video Codecs at the Dial Peer Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. Enter one of the following to configure audio codec:
 - **codec *codec* [bytes *payload-size* fixed-bytes]**
 - **codec isac [mode {adaptive | independent} [bit-rate *value* framesize { 30 | 60 } [fixed]]]**
 - **codec ilbc [mode *frame-size* [bytes *payload-size*]]**
 - **codec mp4-latm [profile *tag*]**
 - **codec opus [profile *tag*]**
5. Add the following to configure a video codec:
 - **video codec *codec***
6. (Optional) Enter one of the following to configure RTP payload type:
 - **rtp payload-type cisco-codec-isac *number***
 - **rtp payload-type cisco-codec-ilbc *number***
 - **rtp payload-type cisco-codec-video-h263+ *number***
 - **rtp payload-type cisco-codec-video-h264 *number***
 - **rtp payload-type opus *number***
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device> configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>number</i> voip Example: Device(config)# dial-peer voice 1 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 4	Enter one of the following to configure audio codec: <ul style="list-style-type: none"> • codec <i>codec</i> [bytes <i>payload-size</i> fixed-bytes] • codec isac [mode {adaptive independent} [bit-rate <i>value</i> framesize { 30 60 } [fixed]]] • codec ilbc [mode <i>frame-size</i> [bytes <i>payload-size</i>]] • codec mp4-latm [profile <i>tag</i>] • codec opus [profile <i>tag</i>] Example: For g711alaw Codec Device(config-dial-peer)# codec g711alaw Example: For ISAC Codec Device(config-dial-peer)# codec isac mode independent	Configures an audio codec at the dial peer level. <ul style="list-style-type: none"> • By default, g729r8, 20-byte payload is configured.
Step 5	Add the following to configure a video codec: <ul style="list-style-type: none"> • video codec <i>codec</i> Example: For h2621 video codec Device(config-dial-peer)# video codec h261	Configures a video codec at the dial peer level.
Step 6	(Optional) Enter one of the following to configure RTP payload type: <ul style="list-style-type: none"> • rtp payload-type cisco-codec-isac <i>number</i> • rtp payload-type cisco-codec-ilbc <i>number</i> • rtp payload-type cisco-codec-video-h263+ <i>number</i> • rtp payload-type cisco-codec-video-h264 <i>number</i> • rtp payload-type opus <i>number</i> Example:	Configures the RTP payload type.

	Command or Action	Purpose
	Device(config-dial-peer)# rtp payload-type opus 114	
Step 7	end Example: Device(config-dial-peer)# end	Returns to privileged EXEC mode.

Verify an Audio Call

SUMMARY STEPS

1. show call active voice [compact]
2. show call active voice [brief]

DETAILED STEPS

Step 1 show call active voice [compact]

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

Example:

```
Router# show call active voice compact
```

```
<callID>  A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 2
          23 ANS   T3      mp4a-latm  VOIP      Psipp              9.45.33.11:57210
          24 ORG   T3      mp4a-latm  VOIP      P123               9.45.33.11:57210
```

Example:

```
Router# show call active voice compact
```

```
<callID>  A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 2
58 ANS    T11          g711ulaw  VOIP      Psipp 2001:.....:230A:6080
59 ORG    T11          g711ulaw  VOIP      P5000110011      10.13.37.150:6090
```

Step 2 show call active voice [brief]

Displays a brief summary of call information for voice calls in progress.

Configuration Examples for Codecs

Example: Configuring a Codec at Dial-Peer Level

```
Device(config)# dial-peer voice 5550199 voip
Device(config-dial-peer)# incoming called-number 5550199
```

```
Device(config-dial-peer)# codec g711ulaw
Device(config-dial-peer)# end
```

Example: Configuring a Codec Preference List and Applying it to a Dial Peer

```
Device(config)# voice class codec 100
Device(config-class)# codec preference 1 g711ulaw
Device(config-class)# exit
Device(config)# dial-peer voice 10 voip
Device(config-dial-peer)# voice-class codec 100
Device(config-dial-peer)# end
```

Example: Configuring a Codec Profile, Codec Preference List and Applying it to a Dial Peer for Opus Codec

```
router(config)#codec profile 79 opus
router(conf-codec-profile)#fmtp "fmtp:114 maxplaybackrate=16000; sprop-maxcapture=16000;
maxaveragebitrate=20000; stereo=1; sprop-stereo=0; useinbandfec=0; usedtx=0"
router(conf-codec-profile)#exit

router(config)#voice class codec 80
router(config-class)#codec preference 1 opus profile 79
router(config-class)#exit

router(config)#dial-peer voice 604 voip
router(config-dial-peer)#rtp payload-type opus 126
router(config-dial-peer)#voice-class codec 80 offer-all
router(config-dial-peer)#exit
```



CHAPTER 9

Call Admission Control

- [Overview](#) , on page 75
- [Configure CAC Based on Total Calls, CPU or Memory](#), on page 76
- [Configure CAC Based on Call Spike Detection](#), on page 77
- [Configure CAC Based on Maximum Calls per Destination](#), on page 78
- [Bandwidth-Based Call Admission Control](#), on page 79

Overview

The Call Admission Control feature enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call Admission Control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time.

The Call Admission Control feature controls number of calls based on resources and bandwidth, proactively reserve resources for good quality video calls, ensures that traffic adheres to QoS policies within each network.

Cisco Unified Border Element (CUBE) provides different CAC mechanisms that are based on:

- Total Calls, CPU, or Memory
- Call Spike Detection
- Maximum Calls per Destination
- Dial-peer or Interface Bandwidth

Feature Information

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 18: Feature Information for Bandwidth-Based Call Admission Control

Feature Name	Releases	Feature Information
Bandwidth-Based Call Admission Control	Baseline Feature	The following commands were introduced or modified: call threshold interface, error-code-override, max-bandwidth, show call threshold, voice-class sip

Configure CAC Based on Total Calls, CPU or Memory

The Call Admission Control (CAC) based on CPU Utilization feature permits the Cisco Voice Gateways to deny incoming calls exceeding a pre-configured threshold, permitting the selection of a system CPU load level value.

The ‘**Call Threshold**’ command allows you to configure two thresholds, high and low. The ‘Call Treatment’ is triggered when the current value of a resource goes beyond the configured high value. The ‘Call Treatment’ remains in effect until the current resource value falls below the configured low value.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call threshold global [cpu-5sec | cpu-avg | io-mem | proc-mem | total-calls | total-mem] low *low-threshold* high *high-threshold***
4. **call treatment on**
5. **end**

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	call threshold global [cpu-5sec cpu-avg io-mem proc-mem total-calls total-mem] low <i>low-threshold</i> high <i>high-threshold</i> Example:	Configures the Call Admission Control feature based on the total calls, cpu, and memory usage at the interface level to reject SIP calls when the bandwidth that is required for the calls exceed the aggregate bandwidth threshold.

	Command or Action	Purpose
	<pre>Device(config)# call threshold global total-calls low 1 high 1 or Device(config)# call threshold global cupu-avg low 75 high 85 or Device(config)# call threshold global toal-mem low 75 high 85</pre>	<p>Note By default, the system rejects incoming calls if the 5 second CPU utilization on the gateway exceeds 95%, and if the in-use process memory on the gateway exceeds 98%.</p>
Step 4	<p>call treatment on</p> <p>Example:</p> <pre>Device(config)# call treatment on</pre>	Enables the call treatment feature.
Step 5	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	Exits global configuration mode and enters privileged EXEC mode.

Example: Internal Error Code (IEC) for Default Call Rejection Based on CPU Utilization and Memory

Following is the sample Internal Error Code (IEC) that explains default call rejection based on CPU utilization and memory:

```
%VOICE_IEC-3-GW: C SCRIPTS: Internal Error (Low memory): IEC=1.1.181.11.4.0 on callID
1GUID=00000000000000000000000000000000
%IVR-3-LOW_MEMORY_RESOURCE: IVR: System running low on memory (99/100 in use). Call (callID=1)
is rejected.

%VOICE_IEC-3-GW: C SCRIPTS: Internal Error (CPU high): IEC=1.1.181.11.3.0 on callID 2
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (97/100). Call
(callID=2) is rejected.

%VOICE_IEC-3-GW: CCAPI: Internal Error (Call spike threshold): IEC=1.1.181.1.29.0 on callID
3
%SIP-3-MEMCAC: Call rejected due to CAC based on Memory usage, sent response 503
```

Configure CAC Based on Call Spike Detection

The Call Admission Control (CAC) based on Call Spike Detection feature permits the Cisco Voice Gateways to monitor call arrival rate over a moving window of time. Calls exceeding the configured rate threshold are rejected. This feature helps in protecting against unexpected high call volumes, and INVITE-based DoS attacks.

You can configure this feature globally or on a per dial-peer level. Error code is sent when a call spike occurs, the error code is configurable globally or on a per dial-peer level.

SUMMARY STEPS

1. enable
2. configure terminal
3. call spike threshold *call number <1-2147483647>steps<3-10> size<100-250>*
4. call treatment on
5. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device>enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	call spike threshold <i>call number <1-2147483647>steps<3-10> size<100-250></i> Example: Device(config)# call spike 10 steps 3 size 100 Device(config)# call spike 12	Configures the Call Spike Call Admission Control feature at the device level to reject SIP calls when the call spike is detected as per the configuration (10 incoming call requests per 300 milliseconds)
Step 4	call treatment on Example: Device(config)# call treatment on	Enables the call treatment feature.
Step 5	end Example: Device(config)# end	Exits global configuration mode and enters privileged EXEC mode.

Configure CAC Based on Maximum Calls per Destination

The Call Admission Control (CAC) based on Maximum Calls per Destination feature permits the Cisco Voice Gateways to restricting the number of concurrent calls that can be active on a VoIP dial peer. Maximum connections work on individual dial-peers and do not provide CAC for the entire gateway.

SUMMARY STEPS

1. enable

2. **configure terminal**
3. **dial-peer voice tag voip**
4. **session protocol sipv2**
5. **max-conn**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# dial-peer voice 10 voip	Enters dial peer voice configuration mode.
Step 4	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures SIP as the session protocol type.
Step 5	max-conn Example: Device(config)# max-conn <1-214748364>	Configures the Maximum Calls per Destination Call Admission Control feature at the device level to allow only 2 toll calls.
Step 6	end Example: Device# end	Exits global configuration mode and enters privileged EXEC mode.

Bandwidth-Based Call Admission Control

The Bandwidth-Based Call Admission Control (CAC) feature provides the functionality to reject SIP calls when the bandwidth accounted by the SIP signaling layer exceeds the aggregate bandwidth threshold for VoIP media traffic—voice, video, and fax. This functionality helps you prevent Quality of Service (QoS) degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized.

Midcall media renegotiation can also be rejected if the configured maximum bandwidth threshold for the VoIP media traffic is exceeded. The call continues as per the previously negotiated media codecs if midcall media renegotiation is rejected.

The excess subscription of the bandwidth allocated for VoIP traffic results in VoIP media packets being dropped or delayed, irrespective of the VoIP call to which they belong. Under such circumstances, it is better to deny new calls to prevent QoS deterioration for existing VoIP call traffic. The existing traffic congestion resolution mechanisms do not differentiate between media packets of existing calls (admitted) and new calls (oversubscribed). Similarly, existing call signaling is unaware of the media traffic congestion. The Bandwidth-Based Call Admission Control feature fills this gap by rejecting new SIP calls when the bandwidth allocated for VoIP traffic is fully utilized. The actual bandwidth usage is not measured and policed. The lower-level QoS policies control the traffic characteristics for the specified traffic class.



Note The Bandwidth-Based Call Admission Control feature is applicable only to VoIP traffic.

Maximum Bandwidth Calculation

The bandwidth requirement for each SIP call leg is calculated using the codec information available in the SDP. Here, the actual media bandwidth used is not measured.

Bandwidth in Kilo bits per second (Kbps) = [codec bytes + RTP header (12) + UDP (8) + IP Header (20 or 40)] * Packets per seconds * 8/1000

Where, codec bytes = Codec payload size, in bytes, for a given packetization interval.

RTP header = Size of the RTP header, in bytes.

UDP = Size of the UDP header, in bytes.

IP Header = Size of the IP header, in bytes. The IPV4 header is 20 bytes and the IPV6 header is 40 bytes.

Packets per second = Number of RTP packets sent or received per second. This value is as per the negotiated packetization interval. The SDP media attribute "ptime" indicates the number of packets per second.

Bandwidth Tables

This section provides the sample maximum bandwidth calculation for audio and fax calls.

Table 19: Audio Bandwidth Table

Codec and Bit Rate (Kbps)	Codec Sample Size in Bytes	Voice Payload Size in Bytes	Voice Payload Size in Milliseconds	Packets Per Second	Bandwidth for IPv4 (excluding Layer 2) in Kbps	Bandwidth for IPv6 (excluding Layer 2) in Kbps
G.711 (64 Kbps)	80	160	20	50	80	88
G.729 (8 Kbps)	10	20	20	50	24	32

G.723.1 (6.3 Kbps)	24	24	30	33.3	17	22
G.723.1 (5.3 Kbps)	20	20	30	33.3	16	21
G.726 (32 Kbps)	20	80	20	50	48	56
G.726 (24 Kbps)	15	60	20	50	40	48
G.726 (16 Kbps)	10	40	20	50	32	40
G.728 (16 Kbps)	10	40	20	50	32	40
G722_64k (64 Kbps)	80	160	20	50	80	88
ilbc_mode_20 (15.2 Kbps)	38	38	20	50	31	39
ilbc_mode_30 (13.33 Kbps)	50	50	30	33.3	24	29
gsm (13 Kbps)	33	33	20	50	30	37
gsm (12 Kbps)	32	32	20	50	29	37
G.Clear (64 Kbps)	80	160	20	50	80	88
GSM AMR	—	—	—	—	15	15
ISAC (32 Kbps)	—	—	—	—	37	37
Aacld (mpeg4)	—	—	—	—	Derived from the SDP bandwidth attribute (TIAS)	Derived from the SDP bandwidth attribute (TIAS)

Table 20: Fax Bandwidth Table

T.38 Fax Bit Rate	Redundancy	Maximum Bandwidth in Kbps
-------------------	------------	---------------------------

2400	None	8
2400	Redundancy	17
9600 (default)	None	16
9600 (default)	Redundancy	46
14400	None	20
14400	Redundancy	65
33600	None	40
33600	Redundancy	142

Restrictions

- CUBE, configured with the Bandwidth-Based Call Admission Control feature, will not reject the call if the bandwidth of the SDP answer is greater than the bandwidth of the SDP offer.
- Layer 2 overhead is not included in the bandwidth calculation.
- A midcall delayed-offer (DO) to DO call is disconnected if the bandwidth requested in an offer message (200 OK) exceeds the threshold bandwidth.
- Real Time Transport Control Protocol (RTCP) and RTP Named phone Event (RTP-NTE) bandwidth requirement is not computed.
- The Bandwidth-Based Call Admission Control feature does not support:
 - Cisco fax relay.
 - Filtering of codecs to accommodate calls within the available bandwidth.
 - Media flow-around, Session Description Protocol (SDP) pass-through, out-of-box low-density transcoding, high-density transcoding, video transcoding, and midcall consumption functionalities.
 - Non-SIP call legs.
 - Subinterfaces for bandwidth-based CAC on an interface.

Configure Bandwidth-Based Call Admission Control

Configure Bandwidth-Based Call Admission Control at the Interface Level

Configure the Bandwidth-Based Call Admission Control feature at the interface level to reject SIP calls when the bandwidth that is required for the call exceeds the aggregate bandwidth threshold.

Configure the Bandwidth-Based Call Admission Control feature for the following interfaces:

- ATM
- Ethernet (Fast Ethernet, Gigabit Ethernet)

- Loopback
- Serial



Note It is recommended that you configure a bind media to associate a specific interface for SIP calls. Otherwise, the interface that is used for the calls is determined based on the best local address that can access the remote media source address (for early offer calls) or the remote signaling source address (for delayed offer calls). When you use a Loopback interface to configure CAC, you must configure an additional bind-to-bind media with the Loopback interface at the global level or the dial peer level. Configure the **bind media source-interface loopback number** command in service SIP configuration mode to configure a bind media.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call threshold interface** *type number int-bandwidth* {**class-map name** [**l2-overhead percentage**] | **low low-threshold high high-threshold**} [**midcall-exceed**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	call threshold interface <i>type number int-bandwidth</i> { class-map name [l2-overhead percentage] low low-threshold high high-threshold } [midcall-exceed] Example: Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth low 1000 high 20000 midcall-exceed or Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth class-map voip-traffic l2-overhead 20 midcall-exceed	Configures the Bandwidth-Based Call Admission Control feature at the interface level to reject SIP calls when the bandwidth that is required for the calls exceed the aggregate bandwidth threshold. <ul style="list-style-type: none"> • You can configure the call threshold interface <i>type number low low-threshold high high-threshold</i> [midcall-exceed] command to apply call admission control to reject SIP calls once the accounted bandwidth reaches the <i>high-threshold</i> value and remains above the <i>low-threshold</i> value. • You can configure the call threshold interface <i>type number int-bandwidth class-map name</i> [l2-overhead percentage] [midcall-exceed] command to use the

	Command or Action	Purpose
		<p>bandwidth value provisioned in the QoS policy under the interface for VoIP media traffic for CAC. See the Modular Quality of Service Command-Line Interface Overview document at http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmdcli.html for information on the usage of the QoS policy with Call Admission Control.</p> <ul style="list-style-type: none"> SIP calls are rejected when the calculated aggregate bandwidth of VoIP media traffic on the specified interface exceeds the configured bandwidth threshold.
Step 4	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	Exits global configuration mode and enters privileged EXEC mode.

Configure Bandwidth-Based Call Admission Control at the Dial Peer Level

You can configure the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth that is required for the calls exceeds the aggregate bandwidth threshold.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *tag* voip**
4. **session protocol sipv2**
5. **max-bandwidth *bandwidth-value* [midcall-exceed]**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>dial-peer voice <i>tag</i> voip</p> <p>Example:</p>	Enters dial peer voice configuration mode.

	Command or Action	Purpose
	Device(config)# dial-peer voice 44 voip	
Step 4	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the Bandwidth-Based Call Admission Control feature for SIP dial peers only.
Step 5	max-bandwidth bandwidth-value [midcall-exceed] Example: Device(config-dial-peer)# max-bandwidth 24 midcall-exceed	Configures the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth that is required for the calls exceed the aggregate bandwidth threshold. <ul style="list-style-type: none"> Configuring the midcall-exceed keyword allows exceeding the bandwidth threshold during mid-call media renegotiation. Media renegotiation exceeding the bandwidth threshold is rejected by default.
Step 6	end Example: Device(config-dial-peer)# end	Exits dial peer configuration mode and enters privileged EXEC mode.

Configure the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping

Mapping of the call rejection cause code to a specific SIP error response code is known as error response code mapping. The cause code for the call rejected because of the bandwidth-based CAC can be mapped to a SIP error response code 400–600. The default SIP error response code is 488.

You can configure SIP error response codes for calls that are rejected by the Bandwidth-Based Call Admission Control feature at the global level, dial peer level, or both.

Configure Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **error-code-override cac-bandwidth failure sip-status-code-number**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

Configure Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice-service configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# sip	Enters service SIP configuration mode.
Step 5	error-code-override cac-bandwidth failure <i>sip-status-code-number</i> Example: Device(conf-serv-sip)# error-code-override cac-bandwidth failure 500	Configures bandwidth-based CAC SIP error response code mapping at the global level.
Step 6	end Example: Device(conf-serv-sip)# end	Exits service SIP configuration mode and enters privileged EXEC mode.

Configure Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag {pots | voatm | vofr | voip}**
4. **voice-class sip error-code-override cac-bandwidth failure {sip-status-code-number | system}**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	dial-peer voice tag {pots voatm vofr voip} Example: Device(config)# <code>dial-peer voice 88 voip</code>	Enters dial peer voice configuration mode.
Step 4	voice-class sip error-code-override cac-bandwidth failure {sip-status-code-number system} Example: Device(config-dial-peer)# <code>voice-class sip error-code-override cac-bandwidth failure 500</code>	Configures bandwidth-based CAC SIP error response code mapping at the dial peer level.
Step 5	end Example: Device(config-dial-peer)# <code>end</code>	Exits dial peer configuration mode and enters privileged EXEC mode.

Verify Bandwidth-Based Call Admission Control

Perform this task to verify the configuration for the Bandwidth-Based Call Admission Control feature on CUBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call threshold config**
3. **show call threshold status**
4. **show call threshold stats**
5. **show dial-peer voice**

DETAILED STEPS

-
- Step 1** **enable**
Example:
 Device>`enable`
 Enables privileged EXEC mode.
- Step 2** **show call threshold config**
Example:

```
Device# show call threshold config

Some resource polling interval:
  CPU_AVG interval: 60
  Memory interval: 5

IF          Type          Value  Low   High  Enable
-----
GigabitEthernet0/0  int-bandwidth  0      100  400   N/A
```

Displays the active call threshold configuration at the interface level for all resources.

Step 3 show call threshold status

Example:

```
Device# show call threshold status

Status  IF          Type          Value  Low   High  Enable
-----
Avail   GigabitEthernet0/0  int-bandwidth  0      100  400   N/A
```

Displays the availability status of resources that are configured when the Bandwidth-Based Call Admission Control feature is enabled at an interface level.

Step 4 show call threshold stats

Example:

```
Device# show call threshold stats

Total resource check: 2
successful: 1
failed: 1

1: -----
Failed resources: int-bandwidth,
related interface: GigabitEthernet0/0; related option:N/A
Recorded time: 04:49:39 UTC Wed Dec 8 2010
2: -----
Successful
All resources are available for this check.
Recorded time: 04:29:39 UTC Wed Dec 8 2010
```

Displays the statistics of resources that are configured when the Bandwidth-Based Call Admission Control feature is enabled at an interface level.

Step 5 show dial-peer voice

Example:

```
Device# show dial-peer voice

incoming called-number = `2000', connections/maximum = 0/unlimited,
bandwidth/maximum = 0/400,
.....
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 3, Refused Calls = 0,
Bandwidth CAC Accepted Calls = 3, Bandwidth CAC Refused Calls = 0
```

Displays information for the voice dial peer.

Tips to Troubleshoot

The following commands can help troubleshoot the Bandwidth-Based Call Admission Control feature:

- `debug ccsip all`
- `debug voice ccapi all`

Configuration Examples for Bandwidth-Based Call Admission Control

Example: Configuring Bandwidth-Based Call Admission Control at the Interface Level

The following example shows how to configure CUBE to reject new SIP calls if the accounted VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds 400 Kbps of bandwidth and continues to have a bandwidth above 100 Kbps:

```
Device> enable
Device# configure terminal
Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth low 100 high
400
```

The following example shows how to configure CUBE to reject new SIP calls if the VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds the configured bandwidth for priority traffic in the “voip_traffic” class:

```
Device>enable
Device# configure terminal
Device(config)# class-map match-all voip-traffic

Device(config-cmap)# policy-map voip-policy
Device(config-pmap)# class voip-traffic
Device(config-pmap-c)# priority 440
Device(config-pmap-c)# end

Device# enaconfigure terminal
Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth class-map
voip-traffic 12-overhead 10
```



Note Layer 2 overhead of 10 percent in the `call threshold` command indicates that the IP bandwidth, excluding Layer 2, is 90 percent of the configured priority bandwidth.

Example: Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level

The following example shows how to configure CUBE to reject calls once the accounted aggregate bandwidth of active calls exceeds 400 Kbps for a SIP dial peer:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2000 voip
Device(config)# session protocol sipv2
Device(config-dial-peer)# max-bandwidth 400
```

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level

The following example shows how to configure CUBE for bandwidth-based CAC SIP error response code mapping at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# error-code-override cac-bandwidth 500
```

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

The following example shows how to configure CUBE for bandwidth-based CAC SIP error response code mapping at the dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 88 voip
Device(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 500
```



CHAPTER 10

SIP Binding

- [Overview](#) , on page 91
- [Configure SIP Binding](#), on page 97
- [Verify SIP Binding](#), on page 99

Overview

The SIP Binding feature enables you to configure a source IP address for signaling packets and media packets.

When you configure SIP on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to an IP address so that only those ports are open to the outside world. In addition, you should protect any public or untrusted interface by configuring a firewall or an Access Control List (ACL) to prevent unwanted traffic from traversing the router.



Note All Cisco Unified Border Element (CUBE) Enterprise deployments must have signaling and media bind statements specified at the dial-peer or voice class tenant level. For Voice class tenants, you must apply tenants to dial-peers used for CUBE call flows if these dial-peers do not have bind statements specified.

Feature Information

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 21: Feature Information for SIP Binding

Feature Name	Releases	Feature Information
Support of Live Binding at dial-peers.	Cisco IOS XE Amsterdam 17.3.1	This feature allows you to either change or add binding on a dial-peer that does not have any active calls, while other dial-peers with the same binding have active calls. The following command was introduced or modified: voice-class sip bind all.

Benefits of SIP Binding

- SIP signaling and media paths can advertise the same source IP address on the gateway for certain applications, even if the paths used different addresses to reach the source. This eliminates confusion for firewall applications that may have taken action on source address packets before the use of binding.
- Firewalls filter messages based on variables such as the message source, the target address, and available ports. Normally a firewall opens only certain addresses or port combination to the outside world and those addresses can change dynamically. Because VoIP technology requires the use of more than one address or port combination, the **bind** command adds flexibility by assigning a gateway to a specific interface (and therefore the associated address) for the signaling or media application.
- You can define specific interface for both signaling and media traffic. The benefits of administrator control are:
 - Administrators know the traffic that runs on specific networks, thereby making debugging easier.
 - Administrators know the capacity of the network and the target traffic, thereby making engineering and planning easier.
 - Traffic is controlled, allowing Quality of Service (QoS) to be monitored.

Source Address

The order of preference for retrieving the SIP signaling and media source address for inbound and outbound calls is as follows:

- Bind configuration at dial peer level
- Bind configuration at tentants
- Bind configuration at global level

The table below describes the state of the system when the **bind** command is applied in the global or dial peer level:

The **bind** command performs different functions based on the state of the interface (see the table below).

Table 22: State of the Interface for the bind Command

Interface State	Result Using Bind Command
Shut down With or without active calls	<p>TCP, TLS, and User Datagram Protocol (UDP) socket listeners are initially closed. (Socket listeners receive datagrams that are addressed to the socket.)</p> <p>Then the sockets are opened to listen to any IP address.</p> <p>If the outgoing gateway has the bind command that is enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.</p> <p>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.</p>
No shut down No active calls	<p>TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams that are addressed to the socket.)</p> <p>Then the sockets are opened and bound to the IP address set by the bind command.</p> <p>The sockets accept packets destined for the bound address only.</p> <p>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.</p>
No shut down Active calls	<p>TCP, TLS, and UDP socket listeners are initially closed.</p> <p>Then the sockets are opened to listen to any IP address.</p> <p>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.</p>
Bound-interface IP address is removed.	<p>TCP, TLS, and UDP socket listeners are initially closed.</p> <p>Then the sockets are opened to listen to any address, because the IP address has been removed. This happens even when SIP was never bound to an IP address.</p> <p>A message stating that the IP address has been deleted from the SIP bound interface is printed.</p> <p>If the outgoing gateway has the bind command that is enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.</p> <p>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.</p>
The physical cable is pulled on the bound port or the interface layer is down.	<p>TCP, TLS, and UDP socket listeners are initially closed.</p> <p>Then the sockets are opened and bound to listen to any address.</p> <p>When the pulled cable is replaced, the result is as documented for no shutdown interfaces.</p> <p>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.</p>

Interface State	Result Using Bind Command
A bind interface is shut down or its IP address is changed or the physical cable is pulled while SIP calls are active.	<p>The call becomes a one-way call with media flowing in only one direction. It flows from the gateway where the change or shutdown took place, to the gateway where no change occurred. Thus, the gateway with the status change no longer receives media.</p> <p>The call is then disconnected, but the disconnected message is not understood by the gateway with the status change, and the call is still assumed to be active.</p> <p>If the bind interface is shut down, the dial peer bind socket listeners of the interface are closed. If the IP address of the interface is changed, the socket listeners representing the bind command is opened with the available IP address of the interface and the configuration turns active for all subsequent SIP messages.</p>



Note If there are active calls, the **bind** command does not take effect if it is issued for the first time or if another **bind** command is in effect. A message reminds you that there are active calls and that the change cannot take effect.

The **bind** command that is applied at the dial peer level can be modified only in the following situations:

Voice Media Stream Processing

If multiple **bind** commands are issued in sequence—That is, if one **bind** command is configured and then another **bind** command is configured—a set interaction happens between the commands. The table below describes the expected command behavior.

Table 23: Interaction Between Previously Set and New bind Commands

Interface State	bind Command	Result Using bind Command
Without active calls	bind all	Generated bind control and bind media commands to override existing bind control and bind media commands.
	bind control	Overrides existing bind control command.
	bind media	Overrides existing bind media command.

Interface State	bind Command	Result Using bind Command
With active calls	bind all or bind control bind media	Global Configuration: Blocks the command, and the following error message appears: <ul style="list-style-type: none"> • Error: You cannot change the interface binding for a dial-peer that is processing live traffic.
	bind all or bind control or bind media	Dial-peer Configuration: You cannot apply bind or no bind command to a dial-peer that is processing active calls. Blocks the command, and the following error message appears: <ul style="list-style-type: none"> • Error: You cannot change the interface binding for a dial-peer that is processing live traffic.

Consider the following scenarios for attaching a tenant to a dial-peer that is processing active calls:

- You can attach a tenant to a dial-peer, when the dial-peer has **bind** (**bind control** or **bind all**) command enabled.
- You cannot attach a tenant to a dial-peer, when the dial-peer has **no bind** or **bind media** command that is enabled and the tenant has **bind control** or **bind all** command enabled.

Consider the following scenarios for changing bind configuration on a tenant, when the tenant is attached to a dial-peer that is processing active calls:

- You can change the bind configuration on tenant, when the associated dial-peer has **bind** (**bind control** or **bind all**) command enabled. Because the dial-peer bind configuration takes precedence over the tenant bind configuration.
- You cannot change the bind configuration on tenant, when the associated dial-peer has **no bind** or **bind media** command that is enabled and the tenant has **bind control** or **bind all** command enabled.

The **bind all** and **bind control** commands perform different functions based on the state of the interface.



Note The **bind all** command applies to global and dial peer. The table below applies to **bind media** only if the media interface is the same as the **bind control** interface. If the two interfaces are different, media behavior is independent of the interface state.

Table 24: bind all and bind control Functions, Based on Interface State

Interface State	Result Using bind all or bind control Commands
Shut down With or without active calls	<p>TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams that are addressed to the socket.)</p> <p>Then the sockets are opened to listen to any IP address.</p> <p>If the outgoing gateway has the bind command that is enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.</p> <p>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.</p>
Not shut down Without active calls	<p>TCP, TLS, and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.)</p> <p>Then the sockets are opened and bound to the IP address set by the bind command.</p> <p>The sockets accept packets that are destined for the bound address only.</p> <p>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.</p>
Not shut down With active calls	<p>TCP, TLS, and UDP socket listeners are initially closed.</p> <p>Then the sockets are opened to listen to any IP address.</p> <p>The dial peer bind socket listeners of the interface are reopened and the configuration turns active for all subsequent SIP messages.</p>
Bound interface's IP address is removed.	<p>TCP, TLS, and UDP socket listeners are initially closed.</p> <p>Then the sockets are opened to listen to any address because the IP address is removed.</p> <p>A message is printed that states the IP address has been deleted from the bound SIP interface.</p> <p>If the outgoing gateway has the bind command that is enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.</p> <p>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.</p>
The physical cable is pulled on the bound port, or the interface layer goes down.	<p>TCP, TLS, and UDP socket listeners are initially closed.</p> <p>Then the sockets are opened and bound to listen to any address.</p> <p>When the pulled cable is replaced, the result is as documented for interfaces that are not shut down.</p> <p>The dial peer bind socket listeners of the interface are closed and the configuration turns inactive for all subsequent SIP messages.</p>

Interface State	Result Using <code>bind all</code> or <code>bind control</code> Commands
A bind interface is shut down, or its IP address is changed, or the physical cable is pulled while SIP calls are active.	<p>The call becomes a one-way call with media flowing in only one direction. The media flows from the gateway where the change or shutdown took place to the gateway where no change occurred. Thus, the gateway with the status change no longer receives media.</p> <p>The call is then disconnected, but the disconnected message is not understood by the gateway with the status change, and the call is still assumed to be active.</p> <p>If the bind interface is shutdown, the dial peer bind socket listeners of the interface are closed. If the IP address of the interface is changed, the socket listeners representing the bind command is opened with the available IP address of the interface and the configuration turns active for all subsequent SIP messages.</p>

Configure SIP Binding

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip address ip-addressmask [secondary]`
5. `exit`
6. Use one of the following commands to configure SIP binding:
 - `bind {control | all} source-interface interface-id [ipv6-address ipv6-address]` in SIP configuration mode.
 - `bind media {source-address ipv4 ipv4-address | source-interface interface-id [ipv6-address ipv6-address]}` in SIP configuration mode.
 - `voice-class sip bind media {source-address ipv4 ipv4-address | source-interface interface-id [ipv6-address ipv6-address]}` in dial-peer configuration mode.
7. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: <pre>Router(config)# interface fastethernet0/0</pre>	Configures an interface type and enters the interface configuration mode. <ul style="list-style-type: none"> • <i>type number</i>—Type of interface to be configured and the port, connector, or interface card number.
Step 4	ip address <i>ip-addressmask</i> [secondary] Example: <pre>Router(config-if)# ip address 192.168.200.33 255.255.255.0</pre>	Configures a primary or secondary IP address for an interface. <p>Note Secondary IP address on an interface with SIP binding is not supported for CUBE.</p>
Step 5	exit Example: <pre>Router(config-if)# exit</pre>	Exits the current mode.
Step 6	Use one of the following commands to configure SIP binding: <ul style="list-style-type: none"> • bind {control all} source-interface <i>interface-id</i> [ipv6-address <i>ipv6-address</i>] in SIP configuration mode. • bind media {source-address ipv4 <i>ipv4-address</i> source-interface <i>interface-id</i> [ipv6-address <i>ipv6-address</i>]} in SIP configuration mode. • voice-class sip bind media {source-address ipv4 <i>ipv4-address</i> source-interface <i>interface-id</i> [ipv6-address <i>ipv6-address</i>]} in dial-peer configuration mode. Example: SIP binding in SIP configuration mode: <pre>Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# bind control source-interface FastEthernet0/0 Device(conf-serv-sip)# exit Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# bind media source-address ipv4 172.18.192.204 Device(conf-serv-sip)# exit</pre> Example: SIP binding in dial-peer configuration mode: <pre>Device(config)# dial-peer voice 100 voip Device(config-dial-peer)# session protocol sipv2 Device(config-dial-peer)# voice-class sip bind</pre>	Sets a source interface for signaling and media packets. The binding applies to the specified interfaces only. SIP must be configured globally or at a dial peer level. <ul style="list-style-type: none"> • control—Binds signaling packets. • media—Binds media packets. • all—Binds signaling and media packets. • source-address—Binds media packets directly to an IP address. • ipv4 <i>ipv4-address</i>—Configures the IPv4 address. • source interface <i>interface-id</i>—Type of interface and its ID. • ipv6-address <i>ipv6-address</i>—Configures the IPv6 address. Ensure that the IPv6 address is applied to an interface.

	Command or Action	Purpose
	<pre>control source-interface fastethernet0/0 Device(config-dial-peer)# exit Device(config)# dial-peer voice 100 voip Device(config-dial-peer)# session protocol sipv2 Device(config-dial-peer)# voice-class sip bind media source-address ipv4 172.18.192.204 Device(config-dial-peer)# exit</pre>	
Step 7	end	Exits to privileged EXEC mode.

Verify SIP Binding

SUMMARY STEPS

1. **show ip sockets**
2. **show sip-ua status**
3. **show sip-ua connections {tcp [tls] | udp} {brief | detail}**
4. **show dial-peer voice**

DETAILED STEPS

Step 1 show ip sockets

Use this command to display IP socket information and indicate whether the bind address of the receiving gateway is set.

The following sample output indicates that the bind address of the receiving gateway is set:

Example:

```
Device# show ip sockets

Proto Remote Port Local Port In Out Stat TTY OutputIF
17 0.0.0.0 0--any-- 2517 0 0 9 0
17 --listen-- 172.18.192.204 1698 0 0 1 0
17 0.0.0.0 0 172.18.192.204 67 0 0 489 0
17 0.0.0.0 0 172.18.192.204 5060 0 0 A1 0
```

Step 2 show sip-ua status

Use this command to display SIP user-agent status and to enable bind.

The following sample output indicates that signaling is disabled and media on 172.18.192.204 is enabled:

Example:

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): ENABLED 172.18.192.204
```

```

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

```

Step 3 **show sip-ua connections {tcp [tls] | udp} {brief | detail}**

Use this command to display the connection details for the UDP transport protocol. The command output looks identical for TCP and TLS.

Example:

```

Device# show sip-ua connections udp detail

Total active connections      : 0
No. of send failures         : 0
No. of remote closures      : 0
No. of conn. failures        : 0
No. of inactive conn. ageouts : 10
-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition
No Active Connections Found
----- SIP Transport Layer Listen Sockets -----
Conn-Id      Local-Address
=====
2            [9.42.28.29]:5060

```

Step 4 **show dial-peer voice**

Use this command, for each dial peer that is configured, to verify that the dial-peer configuration is correct. The following is sample output from this command for a VoIP dial peer:

Example:

```

Device# show dial-peer voice 101

VoiceOverIpPeer1234
  peer type = voice, system default peer = FALSE, information type = voice,
  description = '',
  tag = 1234, destination-pattern = '',

```

```

voice reg type = 0, corresponding tag = 0,
allow watch = FALSE
answer-address = '', preference=0,
CLID Restriction = None
CLID Network Number = ''
CLID Second Number sent
CLID Override RDNIS = disabled,
rtp-ssrc mux = system
source carrier-id = '', target carrier-id = '',
source trunk-group-label = '', target trunk-group-label = '',
numbering Type = 'unknown'
group = 1234, Admin state is up, Operation state is down,
incoming called-number = '', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
modem transport = system,
URI classes:
    Incoming (Request) =
    Incoming (Via) =
    Incoming (To) =
    Incoming (From) =
    Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
outgoing LPCOR:
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = ''
disconnect-cause = 'no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
mailbox selection policy: none
type = voip, session-target = '',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip media rsvp-pass DSCP = ef
ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41, ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
    CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
    A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
    lmr_tone=0, nte_tone=0
    h263+=118, h264=119
    G726r16 using static payload
    G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice, payload size = 20 bytes
fax protocol = system
fax-relay ecm enable

```

```

Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8, payload size = 20 bytes,
video codec = None
voice class codec = ''
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip tel-config url = system,
voice class sip rellxx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number =
    system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
voice class sip block 183 = system,
voice class sip block 181 = system,
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = enabled, 9.42.28.29,
voice class sip bind media = enabled, 9.42.28.29,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number = system,
redirect ip2ip = disabled
local peer = false

```



```
probe disabled,
Secure RTP: system (use the global setting)
voice class perm tag = ``
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
```

Note If the bind address is not configured at the dial-peer, the output of the **show dial-peer voice** command remains the same except for the values of the **voice class sip bind control** and **voice class sip bind media**, which display “system,” indicating that the bind is configured at the global level.

Although the bind all command is an accepted configuration, it does not appear in show running-config command output. Because the bind all command is equivalent to issuing the commands bind control and bind media, those are the commands that appear in the show running-config command output.



CHAPTER 11

Media Path

- [Overview, on page 105](#)
- [Configure Media Flow-Through, on page 107](#)
- [Configure Media Flow-Around, on page 108](#)
- [Configure Media Anti-Tromboning, on page 109](#)

Overview

The Media Path settings determine the path taken by media after a call is established by CUBE.

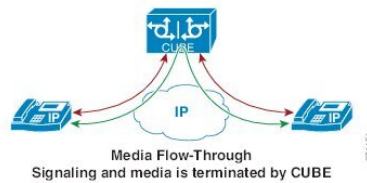


Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

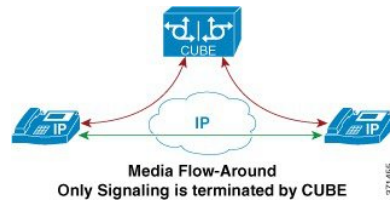
You can configure the media path in the following modes:

- **Media flow-through:** where media and signaling packets terminate and originate on CUBE. As CUBE is an active participant of the call, this mode is recommended when connected outside an enterprise (untrusted endpoints).

Figure 13: Media Flow-Through Mode



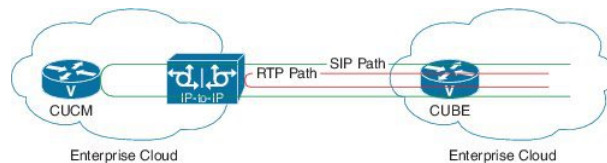
- **Media flow-around:** where signaling packets terminate and originate on CUBE, but media flows directly between endpoints. As media bypasses CUBE, this mode is recommended when connected within an enterprise (trusted endpoints).

Figure 14: Media Flow-Around

- **Media antitrombone:** where CUBE is allowed to detect and avoid loops that are created by call transfers or call forwards. Loops are restricted to the SIP signaling path and removed from the RTP media path.

The user agent may initiate call forwards and call transfers that are sent towards CUBE as a new SIP INVITE dialog. CUBE considers the original call and the forwarded call as separate unrelated calls. Media antitromboning allows CUBE to detect the relation between the calls and resolve the media loop by sending SDP packets back to the sender.

The figure below illustrates how media is needlessly looped over the WAN when loops are not detected.

Figure 15: Tromboning - Needless Looping of Media Packets

The figure below illustrates how CUBE detects and avoids the loop with the antitromboning feature.

Figure 16: Anti-Tromboning - Avoiding Media Loops

- **SDP Pass-Through:** CUBE is configured to pass SDP information transparently, so that both the remote ends can negotiate media independently. SDP pass-through is addressed in two modes:
 - **Flow-through**—CUBE plays no role in media negotiation, it terminates and reoriginates the RTP packets irrespective of the content type that is negotiated by both the ends. This supports address hiding and NAT traversal.
 - **Flow-around**—CUBE neither plays a part in media negotiation, nor does it terminate and reoriginate media. Media negotiation and media exchange is end-to-end.

For more information, refer to the “Configurable Pass-through of SIP INVITE Parameters” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

Restrictions for Media Anti-Tromboning

- Anti-Tromboning is possible for secure (SRTP) calls only when SDP passthrough is enabled.

- Anti-Tromboning is not possible if one call leg is media flow-through and the other call leg is Media Flow-Around. Similarly, antitromboning is not possible if one call leg is configured for Session Description Protocol (SDP) passthrough.

Feature Information

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 25: Feature Information for Configuring Path of Media

Feature Name	Releases	Feature Information
Configuring Media Path	Baseline functionality	The following commands were introduced by this feature: media-flow around, media flow-through, media anti-trombone.

Configure Media Flow-Through

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Use one of the following commands to configure media flow-through:
 - **media flow-through** in dial-peer configuration mode
 - **media flow-through** in global VoIP configuration mode
4. **end**

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	<p>Use one of the following commands to configure media flow-through:</p> <ul style="list-style-type: none"> • media flow-through in dial-peer configuration mode • media flow-through in global VoIP configuration mode <p>Example: In dial-peer configuration mode</p> <pre>! Applying flow-through to one dial peer only Device (config) dial-peer voice 10 voip Device (config-dial-peer) media flow-through Device (config-dial-peer) end</pre> <p>Example: In global VoIP SIP mode</p> <pre>! Applying flow-through globally Device(config)# voice service voip Device(config-voi-serv)#media flow-through Device(config-voi-serv)#end</pre>	Ensures that all media traffic passes through CUBE.
Step 4	end	Exits to privileged EXEC mode.

Configure Media Flow-Around

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Use one of the following commands to configure media flow-around:
 - **media flow-around** in dial-peer configuration mode
 - **media flow-around** in global VoIP configuration mode
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p>	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
Step 3	<p>Use one of the following commands to configure media flow-around:</p> <ul style="list-style-type: none"> • media flow-around in dial-peer configuration mode • media flow-around in global VoIP configuration mode <p>Example: In dial-peer configuration mode</p> <pre>! Applying flow-around to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# media flow-around Device (config-dial-peer)# end</pre> <p>Example: In global VoIP SIP mode</p> <pre>! Applying flow-around globally Device(config)# voice service voip Device(config-voi-serv)#media flow-around Device(config-voi-serv)#end</pre>	Allows media packets to flow directly between endpoints.
Step 4	<code>end</code>	Exits to privileged EXEC mode.

Configure Media Anti-Tromboning

Before you begin

Configure **mode border-element** command under **voice service voip**, global VoIP configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands to configure media antitromboning:
 - **media anti-trombone** in dial-peer configuration mode
 - **media anti-trombone** in global VoIP configuration mode
4. **end**

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	Enter one of the following commands to configure media antitromboning: <ul style="list-style-type: none"> • media anti-trombone in dial-peer configuration mode • media anti-trombone in global VoIP configuration mode Example: In dial-peer configuration mode ! Applying anti-trombone to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# media anti-trombone Device (config-dial-peer)# end Example: In global VoIP SIP mode ! Applying anti-trombone globally Device(config)# voice service voip Device(config-voi-serv)# media anti-trombone Device(config-voi-serv)# end	Enables media anti-trombone for all calls.
Step 4	end	Exits to privileged EXEC mode.



CHAPTER 12

SIP Trunk Monitoring

- [Overview, on page 111](#)
- [Configure SIP Out-of-Dialog OPTIONS Ping Group , on page 114](#)
- [Configure OPTIONS Ping Between CUCM and CUBE, on page 118](#)
- [Additional References, on page 123](#)

Overview

This feature groups the monitoring of SIP dial-peer, endpoints and servers by consolidating dial-peers with the same SIP Out-of-Dialog OPTIONS ping setup.

The SIP Out-Of-Dialog OPTIONS Ping Group feature is an existing mechanism that is used by Cisco Unified Border Element (CUBE) to monitor the status of a single SIP dial-peer destination (keepalive). A generic heartbeat mechanism allows you to monitor the status of SIP servers or endpoints and provide the option of marking a dial peer as inactive (busyout) upon total heartbeat failure.

You can also consolidate the sending of OPTIONS ping packets by grouping dial peers with the same destination. You must create a profile to send one set of OPTIONS ping for a group of dial-peers. If that ping fails, then all of the associated dial-peers are busied out (inactive) by CUBE.



Note Configuring the same Options profile on two or more dial-peers with different bind interfaces configured is not supported. This leads to a scenario wherein the OPTIONS SIP message is not sent from all bind interfaces except the first configured one. But the dial-peer is always marked as ACTIVE. Similarly, it is also not supported in multi VRF setup.

You can use the **shutdown** command to suspend monitoring of all dial peers associated with a keepalive profile.

The command **voice-class sip options-keepalive profile tag** is used to monitor a group of SIP servers or endpoints and the existing **voice-class sip options-keepalive** command is used to monitor a single SIP endpoint or server.

You can configure a server group to be a part of a OPTIONS ping group. A SIP dial peer is updated to BUSY state only if all targets of its server group does not response to the OPTIONS ping. Members of a server group are tested in turn, not in parallel. That is, if the first server group member becomes unavailable, then the second member is tested, and so on. Only when all of the group members are exhausted, is the dial-peer busied out.

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information

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 26: Feature Information for SIP Out-of-dialog OPTIONS Ping Group

Feature Name	Releases	Feature Information
SIP Out-of-dialog OPTIONS Ping Group	Baseline Functionality	This feature groups the monitoring of SIP dial peers endpoints and servers by consolidating SIP Out-Of-Dialog Options of dial peers with the similar OPTIONS ping setup.

OPTIONS Ping for DNS SRV Hosts

From Cisco IOS XE Cupertino 17.9.1a, you can monitor all the SRV hosts that are part of the DNS destination using the OPTIONS Keepalive mechanism. It is therefore possible to load balance calls across all active destinations.

This feature may be used by configuring a dial-peer target with a fully qualified domain name (FQDN) that resolves to a set of DNS SRV records.

A Domain Name System Service Record (DNS SRV) record comprises of multiple resources, each with its own weight, priority and host name. CUBE uses DNS again to resolve the IP address for each of these hostnames. CUBE then triggers an Out-of-Dialog OPTIONS ping to each of these addresses to monitor the status of the hosts.

Once the DNS A query is successful, CUBE triggers an Out-of-Dialog OPTIONS Ping. The Out-of-Dialog OPTIONS Ping mechanism is used by CUBE to monitor the status of the single SIP dial-peer destination (keepalive).

If the DNS lookup returns multiple addresses, then Out-of-Dialog keepalive sessions are established with each of the hosts. For the same destination hostname and the same **voice-class sip options-keepalive profile tag**, only a single Out-of-Dialog OPTIONS SRV entry will be added in the keepalive session table. This SRV entry in the keepalive session table can maintain the session details for each of the hosts.

CUBE compares the least value of Time to Live (TTL) recorded for both SRV resolution and Type A/AAAA resolution. CUBE maintains the least value that is obtained, against the DNS SRV entry in the Out-of-Dialog session table. CUBE starts a periodic timer based on the least TTL value. When the TTL timer expires, the Out-of-Dialog session status is removed for all the existing host entries. Thereafter, CUBE performs a new SRV or Type-A or AAAA lookup to update the DNS SRV entry list.

A generic heartbeat mechanism allows you to monitor the status of SIP servers or endpoints. It provides the option of marking a dial-peer as **active**, inactive (**busyout**) for a total heartbeat failure, and partially active (**partial**). A dial-peer is marked as partially active if at least one of the destinations is active out of a group, and the rest are inactive (busyout). A dial-peer is marked as busyout, only if all the destinations in the dial-peer have a heartbeat failure and fail to respond.

Once OPTIONS Ping is successful, this destination is considered for the routing of call handling. CUBE monitors all the destinations irrespective of the response (503, 200 OK, and so on) that it receives. Based on the response, CUBE identifies the destination that it can communicate with. If CUBE receives a 503 response or no response for the INVITE, CUBE then marks that destination as busyout and attempts call on the next destination that is marked as active. The call is rejected if all possible destinations are busy out.



-
- Note**
- If Outbound Proxy is configured on dial-peer or a tenant that is associated with the dial-peer, CUBE maintains keepalive session with the Outbound Proxy address.
 - You need to configure the same transport type for the dial-peers with same SRV destination.
-

You must configure **voice-class sip options-keepalive profile <tag>** under the specific **dial-peer** to support the DNS SRV lookup using the OPTIONS keepalive mechanism. If you configure the **voice-class sip options-keepalive** command under the dial-peer, Load Balancing using DNS SRV is not supported.



-
- Note** We recommended that you configure the same **voice-class sip options-keepalive profile <tag>** under all dial-peers that have the same DNS session target. This helps to reduce the OPTIONS Ping traffic.
-

To display the status of the destination when options-keepalive is configured under dial-peer, use the CLI command **show dial-peer voip keepalive status <dp-tag> | tenant <tenant-id> | <cr>**. The options keepalive status is maintained by CUBE for individual session targets and server groups in this command. The keepalive status is displayed for IPv4, IPv6, and DNS format destinations.

The CLI command **show dial-peer voice summary** is enhanced to display the overall keepalive status for the DNS SRV at the dial-peer level.

To display the status of session target DNS with the list of servers resolved against the DNS SRV records, use the CLI command **show voice class sip-options-keepalive <profile-tag>**.

Load Balancing for DNS SRV Hosts

The usage of DNS SRV as the target for CUBE helps in load balancing of the outbound SIP call traffic across the trunk. Based on the priority, weight, and status of the DNS SRV records, the multiple hosts associated with DNS SRV are used. CUBE distributes calls across the SRVs based on the priority and status of the DNS SRV records.

During call routing, CUBE reads through the DNS SRV records that it has collected. Based on the information, CUBE identifies the trunk dial-peer destinations that are still available. Based on this, CUBE can distribute the traffic of outbound SIP calls in a more efficient way.

If configured, CUBE uses the Out-of-Dialog OPTIONS Ping mechanism to monitor the status of the hosts defined by the dial-peer destination SRV record. For more information on OPTIONS Ping for DNS SRV hosts, see [OPTIONS Ping for DNS SRV Hosts, on page 112](#).

Configure SIP Out-of-Dialog OPTIONS Ping Group

Before you begin

Configure SIP profiles and server groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-options-keepalive** *keepalive-group-profile-id*
4. **description** *text*
5. **transport {tcp [tls] | udp | system}**
6. **sip-profiles** *profile-number*
7. **down-interval** *down-interval*
8. **up-interval** *up-interval*
9. **retry** *retry-interval*
10. **exit**
11. **dial-peer voice** *dial-peer-id* **voip**
12. **session protocol sipv2**
13. **voice-class sip options-keepalive profile** *keepalive-group-profile-id*
14. **session server-group** *server-group-id*
15. **end**
16. **show voice class sip-options-keepalive** *keepalive-group-profile-id*

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class sip-options-keepalive <i>keepalive-group-profile-id</i> Example: Device(config)# voice class sip-options-keepalive 171	Configures a keepalive profile and enters voice class configuration mode. <ul style="list-style-type: none"> You can use the shutdown command to suspend keepalive activity for all dial peers associated with the keepalive profile.
Step 4	description <i>text</i> Example: Device(config-class)# description Target Boston	Configures a textual description for the keepalive heartbeat connection.
Step 5	transport {tcp [tls] udp system} Example: Device(config-class)# transport tcp	Defines the transport protocol that is used for the keepalive heartbeat connection. <ul style="list-style-type: none"> The default value is system.
Step 6	sip-profiles <i>profile-number</i> Example: Device(config-class)# sip-profiles 100	Specifies the SIP profile that is to be used to send this message. <ul style="list-style-type: none"> To configure a SIP profile, refer to “Configuring SIP Parameter Modification”.
Step 7	down-interval <i>down-interval</i> Example: Device(config-class)# down-interval 35	Configures the time (in seconds) at which an OPTIONS ping is sent to the dial-peer endpoint when the heartbeat connection to the endpoint is in Down status. <ul style="list-style-type: none"> The default value is 30.
Step 8	up-interval <i>up-interval</i> Example: Device(config-class)# up-interval 65	Configures the time (in seconds) at which an OPTIONS ping is sent to the dial-peer endpoint when the heartbeat connection to the endpoint is in Up status. <ul style="list-style-type: none"> The default value is 60.
Step 9	retry <i>retry-interval</i> Example: Device(config-class)# retry 30	Configures the maximum number of OPTIONS ping retries that are permitted for a dial-peer destination. After receiving failed responses for the configured number of OPTIONS pings, the heartbeat connection status should be switched from Up to Down. <ul style="list-style-type: none"> The default value is 5. If a successful response is received for an OPTIONS ping, the retry counter is set to zero.

	Command or Action	Purpose
Step 10	exit Example: Device(config-class)# exit	Exits voice class configuration mode and enters global configuration mode.
Step 11	dial-peer voice <i>dial-peer-id</i> voip Example: Device(config)# dial-peer voice 123 voip	Defines a local dial peer and enters dial peer configuration mode.
Step 12	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Specifies SIP version 2 as the session protocol for calls between local and remote routers using the packet network.
Step 13	voice-class sip options-keepalive profile <i>keepalive-group-profile-id</i> Example: Device(config-dial-peer)# voice-class sip options-keepalive profile 171	Associates the dial peer with the specified keepalive group profile. The dial peer is monitored by CUBE according to the parameters defined by this profile.
Step 14	session server-group <i>server-group-id</i> Example: Device(config-dial-peer)# session server-group 151	Associates the dial peer with the specified keepalive group profile. The dial peer is monitored by the device according to the parameters defined by this profile.
Step 15	end Example: Device(config-dial-peer)# end	Exits dial peer configuration mode and enters privileged EXEC mode.
Step 16	show voice class sip-options-keepalive <i>keepalive-group-profile-id</i> Example: Device# show voice class sip-options-keepalive 171	Displays information about voice class server group.

Configuration Examples For SIP Out-of-Dialog OPTIONS Ping Group

Example: SIP Out-of-Dialog OPTIONS Ping for Group of SIP Endpoints

```
!Configuring the SIP profile
Device(config)# voice class sip-profiles 100
Device(config-class)# request OPTIONS sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
```

```

!Configuring the SIP Keepalive Group
Device(config)# voice class sip-options-keepalive 171
Device(config-class)# transport tcp
Device(config-class)# sip-profile 100
Device(config-class)# down-interval 30
Device(config-class)# up-interval 60
Device(config-class)# retry 5
Device(config-class)# description Target New York
Device(config-class)# exit

!Configuring an outbound SIP Dial Peer
Device(config)# dial-peer voice 123 voip
Device(config-dial-peer)# session protocol sipv2
!Associating the Dial Peer with a keepalive profile group
Device(config-dial-peer)# session target dns:example.com
Device(config-dial-peer)# voice-class sip options-keepalive profile 171
Device(config-dial-peer)# end

!Verifying the Keepalive group configurations
Device# show voice class sip-options-keepalive 171

Voice class sip-options-keepalive: 171           AdminStat: Up
Description: Target New York
Transport: system                               Sip Profiles: 100
Interval(seconds) Up: 60                       Down: 30
Retry: 5

  Peer Tag      Server Group      OOD SessID      OOD Stat      IfIndex
  -----      -
  123

```

Example: SIP Out-of-dialog OPTIONS Ping for Group of SIP Servers

```

!Configuring the Server Group
Device(config)# voice class server-group 151
Device(config-class)# ipv4 10.1.1.1 preference 1
Device(config-class)# ipv4 10.1.1.2 preference 2
Device(config-class)# ipv4 10.1.1.3 preference 3
Device(config-class)# hunt-scheme round-robin
Device(config-class)# description It has 3 entries
Device(config-class)# exit

!Configuring an E164 pattern map class
Device(config)# voice class e164-pattern-map 3000
Device(config-class)# e164 300

!Configuring an outbound SIP dial peer.
Device(config)# dial-peer voice 181 voip
!Associate a destination pattern map
Device(config-dial-peer)# destination e164-pattern-map 3000
Device(config-dial-peer)# session protocol sipv2
!Associate a server group with the dial peer
Device(config-dial-peer)# session server-group 151
!Associate the dial peer with a keepalive profile group
Device(config-dial-peer)# voice-class sip options-keepalive profile 171
Device(config-dial-peer)# end

!Verifying the Keepalive group configurations
Device# show voice class sip-options-keepalive 171

```

```

Voice class sip-options-keepalive: 171          AdminStat: Up
Description: Target New York
Transport: system                               Sip Profiles: 100
Interval(seconds) Up: 60                       Down: 30
Retry: 5

Peer Tag      Server Group  OOD SessID  OOD Stat  IfIndex
-----      -
123
181          151          Busy        106

Server Group: 151          OOD Stat: Busy
OOD SessID  OOD Stat
-----
1           Busy
2           Busy
3           Busy

OOD SessID: 1          OOD Stat: Busy
Target: ipv4:10.1.1.1  Sip Profiles: 100
Transport: system

OOD SessID: 2          OOD Stat: Busy
Target: ipv4:10.1.1.2  Sip Profiles: 100
Transport: system

OOD SessID: 3          OOD Stat: Busy
Target: ipv4:10.5.0.1  Sip Profiles: 100
Transport: system
-----

```

Configure OPTIONS Ping Between CUCM and CUBE

This section describes how to enable Options Ping between Cisco Unified Communications Manager (CUCM) and Cisco Unified Border Element (CUBE).



The following figure describes how a CUCM extends a call out of a SIP Trunk:

SIP Information

Destination

Destination Address is an SRV

Destination Address

1* 192.168.1.57

The following figure shows the TCP three-way handshake in Wireshark:

Source	Destination	Protocol	Length	Info
192.168.1.26	192.168.1.57	TCP	74	38672 → 5068 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1
192.168.1.57	192.168.1.26	TCP	60	5068 → 38672 [SYN, ACK] Seq=0 Ack=1 Win=128 Len=0 MSS=1460
192.168.1.26	192.168.1.57	TCP	54	38672 → 5068 [ACK] Seq=1 Ack=1 Win=14600 Len=0
192.168.1.26	192.168.1.57	SIP	1271	Request: [INVITE sip:5123@192.168.1.57:5060]

Perform the following steps to configure OPTIONS ping between CUBE and CUCM:

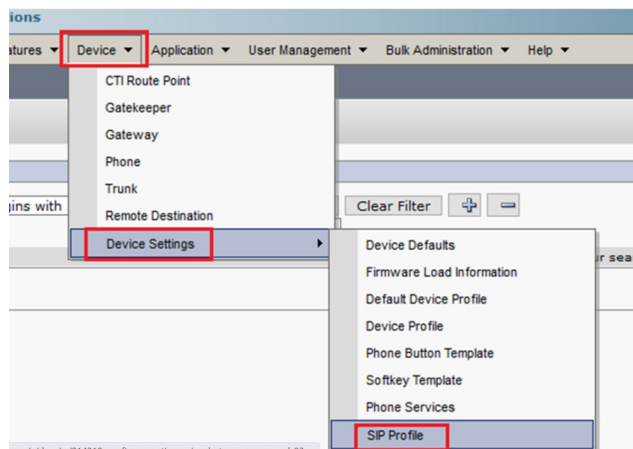
SUMMARY STEPS

1. Enable SIP Options Ping in the **SIP Profile Configuration**:
2. Add the SIP profile to the SIP trunk and click **Save**:
3. Enable SIP Options Ping on the far end of the SIP Trunk. In this case, 192.X.X.57 (ISR 4351).

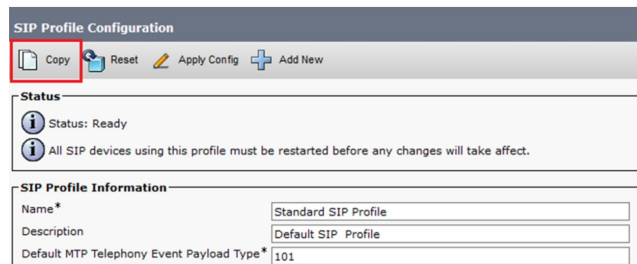
DETAILED STEPS

Step 1 Enable SIP Options Ping in the SIP Profile Configuration:

- a) Navigate to **Cisco Unified CM Administration >> Device >> Device Settings >> SIP Profile** as shown in the following figure:



- b) Click **find** and decide if you want to create a new **SIP Profile**, edit a **SIP Profile** that exists or make a copy of a SIP Profile. For this example, create a copy of the **Standard SIP Profile** as shown in the following figures:



- c) Rename the new SIP Profile and enable the OPTIONS Ping option as shown in the following figure:

Configure OPTIONS Ping Between CUCM and CUBE

SIP Profile Configuration

Save

Status
 Status: Ready
 All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name* Options Ping SIP Profile
 Description Default SIP Profile
 Default MTP Telephony Event Payload Type* 101
 Early Offer for G.Clear Calls* Disabled
 User-Agent and Server header information* Send Unified CM Version Information as User-Agen
 Version in User Agent and Server Header* Major And Minor
 Dial String Interpretation* Phone number consists of characters 0-9, *, #, anc
 Confidential Access Level Headers* Disabled

SIP OPTIONS Ping
 Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"
 Ping Interval for In-service and Partially In-service Trunks (seconds)* 60

Step 2 Add the SIP profile to the SIP trunk and click **Save**:

Cisco Unified CM Administration
 For Cisco Unified Communications Solutions

Call Routing | Media Resources | Advanced Features | **Device** | Application | User Management

Device Configuration

Delete | Copy | Reset | Apply Config

successful
 SIP devices using this profile must be restarted before any

Device Information

Name Options Ping SIP Profile
 Description Default SIP Profile
 MTP Telephony Event Payload Type* 101
 Offer for G.Clear Calls* Disabled
 User-Agent and Server header information* Send Unified CM Version Information as User-Agen
 User Agent and Server Header* Major And Minor
 Dial String Interpretation* Phone number consists of characters 0-9, *, #, anc

Find and List Trunks

Add New | Select All | Clear All | Delete Selected | Reset Selected

Status
 1 records found

Trunks (1 - 1 of 1)

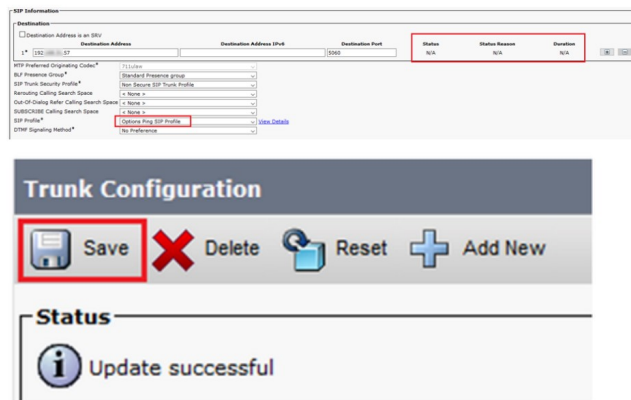
Find Trunks where Device Name | begins with | TAC | Find
 Select item or enter search text

	Name ^	Description	Calling Search Space
<input type="checkbox"/>	TAC-SIP-Trunk	TAC SIP Trunk	

- Note**
- You must have previously configured this trunk. See [System Configuration Guide](#).
 - Set **Status**, **Status Reason**, and **Duration** to N/A.

- Navigate to **Device >> Trunk**.
- Choose the correct SIP profile and click **Save**.

- Note**
- You must reset the trunk after saving for the changes to take effect.
 - The reset disconnects active calls and does not allow any incoming calls for a short time.



- c) Monitor the status of the **SIP Trunk** in Cisco Unified Communications Manager.



Step 3

Enable SIP Options Ping on the far end of the SIP Trunk. In this case, 192.X.X.57 (ISR 4351).

- a) Navigate to the ISR CUBE or Gateway and confirm what dial-peer you want to add the Options Ping to as shown in the following figure:

```
ISR4351#show running-config | s voice 100
dial-peer voice 100 voip
description CUCM Dial-Peer
session protocol sipv2
session target ipv4:192.x.x.26
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

- b) Add Options Ping with the command: voice-class sip options-keepalive using a profile.

```
dial-peer voice 100 voip
description CUCM Dial-Peer
session protocol sipv2
session target ipv4:192.x.x.26
voice-class sip options-keepalive profile 1
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

What to do next

Verify

Confirm that Options messages are exchanged correctly in this section.



Note To understand how to run a packet capture on CUCM eth0 port, follow the instructions in this link: [Packet Capture on CUCM Appliance Model](#).

- The TCP three-way handshake is only done once, when you restart the trunk. Afterwards, you only have OPTIONS messages that are sent from CUCM to ISR where you expect a 200 OK as a response. These messages are exchanged every 60 seconds by default.

Source	Destination	Protocol	Length	Info
192.168.1.26	192.168.1.57	TCP	74	46535 → 5060 [SYN] Seq=0 Win=14600 Len=0 MSS=1460
192.168.1.57	192.168.1.26	TCP	60	5060 → 46535 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
192.168.1.26	192.168.1.57	TCP	54	46535 → 5060 [ACK] Seq=1 Ack=1 Win=14600 Len=0
192.168.1.26	192.168.1.57	SIP	451	Request: OPTIONS sip:192.168.1.57:5060
192.168.1.57	192.168.1.26	TCP	60	5060 → 46535 [ACK] Seq=1 Ack=398 Win=3731 Len=0
192.168.1.57	192.168.1.26	SIP/SDP	1014	Status: 200 OK

- Options messages are only sent from 192.X.X.26 (CUCM) to 192.X.X.57 (ISR) because only CUCM is configured to monitor the trunk status:

Time	Source	Destination	Protocol	Length	Info
13:37	46.829581	192.168.1.26	192.168.1.57	SIP	451 Request: OPTIONS sip:192.168.1.57:5060
13:37	46.031672	192.168.1.57	192.168.1.26	SIP/SDP	1014 Status: 200 OK
13:38	47.552245	192.168.1.26	192.168.1.57	SIP	451 Request: OPTIONS sip:192.168.1.57:5060
13:38	47.554691	192.168.1.57	192.168.1.26	SIP/SDP	513 Status: 200 OK
13:39	48.095232	192.168.1.26	192.168.1.57	SIP	452 Request: OPTIONS sip:192.168.1.57:5060
13:39	48.097399	192.168.1.57	192.168.1.26	SIP/SDP	1014 Status: 200 OK
13:40	50.418479	192.168.1.26	192.168.1.57	SIP	451 Request: OPTIONS sip:192.168.1.57:5060
13:40	50.420957	192.168.1.57	192.168.1.26	SIP/SDP	1014 Status: 200 OK
13:41	51.014881	192.168.1.26	192.168.1.57	SIP	451 Request: OPTIONS sip:192.168.1.57:5060
13:41	51.017117	192.168.1.57	192.168.1.26	SIP/SDP	1013 Status: 200 OK
13:42	52.389610	192.168.1.26	192.168.1.57	SIP	451 Request: OPTIONS sip:192.168.1.57:5060

- When you call, CUCM already knows that the trunk is in an operational status and sends an invite:

Time	Source	Destination	Protocol	Length	Info
192.168.1.57	192.168.1.26	SIP/SDP	1013	Status: 200 OK	
192.168.1.26	192.168.1.57	SIP	451	Request: OPTIONS sip:192.168.1.57:5060	
192.168.1.57	192.168.1.26	SIP/SDP	1013	Status: 200 OK	
192.168.1.26	192.168.1.57	SIP	1271	Request: INVITE sip:5123@192.168.1.57:5060	

- If you have completed Step 3 configuration on CUBE, you see that Options messages sent both ways:

Time	Source	Destination	Protocol	Length	Info
192.168.1.57	192.168.1.26	SIP/SDP	1013	Status: 200 OK	
192.168.1.26	192.168.1.57	SIP	451	Request: OPTIONS sip:192.168.1.57:5060	
192.168.1.57	192.168.1.26	SIP/SDP	1013	Status: 200 OK	
192.168.1.26	192.168.1.57	SIP	1271	Request: INVITE sip:5123@192.168.1.57:5060	

Troubleshoot

To troubleshoot Options Ping in CUCM, you need:

- Start with Packet Captures from CUCM Eth0 port. For more details, [Packet Capture on CUCM Appliance Model](#).
- Check detailed Cisco Call Manager traces. Download them with RTMT. See the steps here: [How to Collect Traces for CUCM 9.x or Later](#)
- Verify the SIPTrunkOOS Reason codes in this link: [System Error Message](#).
 - Local=1 (request timeout)
 - Local=2 (local SIP stack is not able to create a socket connection with the remote peer)
 - Local=3 (DNS query failed)

To troubleshoot Options Ping in CUBE, you need the following:

- **debug ccsip messages**
- **debug ccsip non-call**

- **debug voip ccapi inout**
- Packet captures from an interface that point toward CUCM.

Additional References

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS Commands	Cisco IOS Command List, All Releases
SIP Configuration Guide	
Configuring SIP profiles	
Configuring server groups	



CHAPTER 13

VoIP for IPv6

- [Overview](#), on page 125
- [Prerequisites](#), on page 131
- [Restrictions](#), on page 131
- [Configure SIP for IPv6](#), on page 131

Overview

This document describes VoIP in IPv6, and dual-stack (IPv4 and IPv6) interworking.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 27: Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
CUBE support for IPv6	Baseline Functionality	The feature supports interworking for SIP IPv4-IPv6 dual stack and IPv4 and IPv6.

IPv6 SIP Features

A SIP User Agent (UA) operates in one of the following three modes:

- IPv4-only: Communication with only IPv6 UA is unavailable.
- IPv6-only: Communication with only IPv4 UA is unavailable.
- Dual-stack: Communication with only IPv4, only IPv6 and dual-stack UAs are available.

SIP Protocol Handling for VoIPv6

In addition to the already existing features that are supported on IPv4 and IPv6, the SIP Voice Gateways support the following features:

- **History–Info:** The SIP History–info Header Support feature provides support for the history-info header in SIP INVITE messages only. The SIP gateway generates history information in the INVITE message for all forwarded and transferred calls. The history-info header records the call or dialog history. The receiving application uses the history-info header information to determine how and why the call has reached it.

For more information, refer to the “SIP History INFO” section in the [Cisco Unified Border Element \(Enterprise\) SIP Support Configuration Guide](#).

- **Handling 181/183 Responses with/without SDP:** The Handling 181/183 Responses with/without SDP feature provides support for SIP 181 (Call is Being Forwarded) and SIP 183 (Session Progress) messages either globally or on a specific dial-peer. Also, you can control when the specified SIP message is dropped based on either the absence or presence of SDP information.

For more information, refer to “SIP–Enhanced 180 Provisional Response Handling” section in the [Cisco Unified Border Element Configuration Guide](#).

- **Limiting the Rate of Incoming SIP Calls per Dial-Peer (Call Spike):** The call rate-limiting feature for incoming SIP calls starts working after a switch over in a SIP call. The rate-limiting is done for incoming calls that are received on the new Active. The IOS timers that track the call rate limits runs on Active and Standby mode and does not require any checkpoint. However, some statistics for calls that are rejected requires to be checked for the show commands to be consistent before and after the switchover.

- **PPI/PAI/Privacy and RPID Passing:** For incoming SIP requests or response messages, when the PAI or PPI privacy header is set, the SIP gateway builds the PAI or PPI header into the common SIP stack, thereby providing support to handle the call data present in the PAI or PPI header. For outgoing SIP requests or response messages, when the PAI or PPI privacy header is set, privacy information is sent using the PAI or PPI header.

For more information, refer to the “Support for PAID PPID Privacy PCPID and PAURI Headers on CUBE” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

- **SIP Session timer (RFC 4028):** This feature allows for a periodic refresh of SIP sessions through a re-INVITE or UPDATE request. The refresh allows both user agents and proxies to determine whether the SIP session is still active. Two header fields can be defined: Session-Expires, which conveys the lifetime of the session, and Min-SE, which convey the minimum allowed value for the session timer.

For more information, refer to the “SIP Session Timer Support” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

- **SIP Media Inactivity Detection:** The SIP Media Inactivity Detection Timer feature enables Cisco gateways to monitor and disconnect VoIP calls if no Real-Time Control Protocol (RTCP) packets are received within a configurable time period.

For more information, refer to the [SIP Media Inactivity Timer](#) section.

VoIPv6 Support

This feature adds dual-stack support IPv6 support for SIP trunks, support for real-time control protocol (RTCP) pass-through, and support for T.38 fax over IPv6.

For more information on these features, refer to the following:

- “Configuring Cisco IOS Gateways” section in the [Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager](#)
- “Trunks” section in the [Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager](#)
- “RTCP Pass-Through” section in [Cube RTCP Voice Pass-Through for IPv6](#)
- “T.38 fax over IPv6” section in [Fax, Modem, and Text Support over IP Configuration Guide](#)
- The feature supports for audio calls in media Flow-Through (FT) and Flow-Around (FA) modes, Local Transcoding Interface (LTI), along with Voice Class Codec (VCC) support, support for Hold/Resume, REFER, re-INVITE, 302 based services, and support for media anti-trombone have been added to CUBE.

CUBE being a signaling proxy processes all signaling messages for setting up media channels. This enables CUBE to affect the flow of media packets using the media flow-through and the media flow-around modes.

- Media FT and Media FA modes support the following call flows:
 - EO-to-EO
 - DO-to-DO
 - DO-to-EO
- **Media Flow-Through (FT):** In a media flow-through mode, between two endpoints, both signaling and media flows.
- **Media Flow-Around (FA):** Media flow-around provides the ability to have a SIP video call whereby signaling passes through CUBE and media pass directly between endpoints bypassing the CUBE.
- **SDP Pass-Through:** SDP is configured to pass through transparently at the CUBE, so that both the remote ends can negotiate media independently of the CUBE.

SDP pass-through is addressed in two modes:

- Flow-through—CUBE plays no role in the media negotiation, it blindly terminates and re-originates the RTP packets irrespective of the content type negotiated by both the ends. This supports address hiding and NAT traversal.
- Flow-around—CUBE neither plays a part in media negotiation, nor does it terminate and re-originate media. Media negotiation and media exchange is completely end-to-end.

For more information, refer to the “Configurable Pass-through of SIP INVITE Parameters” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#) .

- **UDP Checksum for IPv6:** User Datagram Protocol (UDP) checksums provide data integrity for addressing different functions at the source and destination of the datagram, when a UDP packet originates from an IPv6 node.

- **IP Toll Fraud:** The IP Toll Fraud feature checks the source IP address of the call setup before routing the call. If the source IP address does not match an explicit entry in the configuration as a trusted VoIP source, the call is rejected.

For more information, refer to the “Configuring Toll Fraud Prevention” section in the [Cisco Unified Communications Manager Express System Administrator Guide](#).

- **RTP Port Range:** Provides the capability where the port range is managed per IP address range. This feature solves the problem of limited number of RTP ports for more than 4000 calls. It enables combination of an IP address and a port as a unique identification for each call.
- **Hold/Resume:** CUBE supports supplementary services such as Call Hold and Resume. An active call can be put in held state and later the call can be resumed.

For more information, refer to the “Configuring Call Hold/Resume for Shared Lines for Analog Ports” section in [Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide](#).

- **Call Transfer (re-INVITE, REFER):** Call transfer is used for conference calling, where calls can transition smoothly between multiple point-to-point links and IP level multicasting.

For more information, refer to the “Configurable Pass-through of SIP INVITE Parameters” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

- **Call Forward (302 based):** SIP provides a mechanism for forwarding or redirecting incoming calls. A Universal Access Servers (UAS) can redirect an incoming INVITE by responding with a 302 message (moved temporarily).
 - Consumption of 302 at stack level is supported for EO-EO, DO-DO and DO-EO calls for all combination of IPv4/IPv6/ANAT.
 - Consumption of 302 at stack level is supported for both FT and FA calls.

For more information, refer to the “Configuring Call Transfer and Forwarding” section in [Cisco Unified Communications Manager Express System Administrator Guide](#).

- **Media Antitrombone:** Antitromboning is a media signaling service in SIP entity to overcome the media loops. Media Trombones are media loops in a SIP entity due to call transfer or call forward. Media loops in CUBE are not detected because CUBE looks at both call types as individual calls and not calls related to each other.

Antitrombone service has to be enabled only when no media interworking is required in both legs. Media antitrombone is supported only when the initial call is in IPv4 to IPv4 or IPv6 to IPv6 mode only.

For more information, refer to the “Configuring Media Antitrombone” section in the [Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide](#).

- **RE-INVITE Consumption:** The Re-INVITE/UPDATE consumption feature helps to avoid interoperability issues by consuming the mid-call Re-INVITES/UPDATES from CUBE. As CUBE blocks RE-INVITE / mid-call UPDATE, remote participant is not made aware of the SDP changes, such as Call Hold, Call Resume, and Call transfer.

For more information, refer to the “CUBE Mid-call Re-INVITE/UPDATE Consumption” section in the [Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide](#).

- **Address Hiding:** The address hiding feature ensures that the CUBE is the only point of signaling and media entry/exit in all scenarios. When you configure address-hiding, signaling and media peer addresses

are also hidden from the endpoints, especially for supplementary services when the CUBE passes REFER/3xx messages from one leg to the other.

For more information, refer to the “Configuring Address Hiding” section in the [SIP-to-SIP Connections on a Cisco Unified Border Element](#).

- **Header Passing:** Header Pass through enables header passing for SIP INVITE, SUBSCRIBE and NOTIFY messages; disabling header passing affects only incoming INVITE messages. Enabling header passing results in a slight increase in memory and CPU utilization.

For more information, refer to the “SIP-to-SIP Connections on a Cisco Unified Border Element” section in the [SIP-to-SIP Connections on Cisco Unified Border Element](#).

- **Refer-To Passing:** The Refer-to Passing feature is enabled when you configure refer-to-passing in Refer Pass through mode and the supplementary service SIP Refer is already configured. This enables the received refer-to header in Refer Pass through mode to move to the outbound leg without any modification. However, when refer-to-passing is configured in Refer Consumption mode without configuring the supplementary-service SIP Refer, the received Refer-to URI is used in the request-URI of the triggered invite.

For more information, refer to the “Configuring Support for Dynamic REFER Handling on CUBE” section in the [Cisco Unified Border Element SIP Configuration Guide](#).

- **Error Pass-through:** The SIP error message pass through feature allows a received error response from one SIP leg to pass transparently over to another SIP leg. This functionality will pass SIP error responses that are not yet supported on the CUBE or will preserve the Q.850 cause code across two sip call-legs.

For more information, refer to the “Configuring SIP Error Message Passthrough” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

- **SIP UPDATE Interworking:** The SIP UPDATE feature allows a client to update parameters of a session (such as, a set of media streams and their codecs) but has no impact on the state of a dialog. UPDATE with SDP will support SDP Pass through, media flow around and media flow through. UPDATE with SDP support for SIP to SIP call flows is supported in the following scenarios:

- Early Dialog SIP to SIP media changes.
- Mid Dialog SIP to SIP media changes.

For more information, refer to the “SIP UPDATE Message per RFC 3311” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

- **SIP OPTIONS Ping:** The OPTIONS ping mechanism monitors the status of a remote Session Initiation Protocol (SIP) server, proxy or endpoints. CUBE monitors these endpoints periodically.

For more information, refer to the “CUBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints” section in the [Configuration of SIP Trunking for PSTN Access \(SIP-to-SIP\) Configuration Guide](#).

- **Configurable Error Response Code in OPTIONS Ping:** CUBE provides an option to configure the error response code when a dial peer is busied out because of an Out-of-Dialog OPTIONS ping failure.

For more information, refer to the “Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure” section in the [Cisco Unified Border Element SIP Support Configuration Guide](#).

- **SIP Profiles:** SIP profiles create a set of provisioning properties that you can apply to SIP trunk.

- **Dynamic Payload Type Interworking (DTMF and Codec Packets):** The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for dual tone multifrequency (DTMF) and codec packets for Session Initiation Protocol (SIP) to SIP calls. The CUBE interworks between different dynamic payload type values across the call legs for the same codec. Also, CUBE supports any payload type value for audio, video, named signaling events (NSEs), and named telephone events (NTEs) in the dynamic payload type range 96 to 127.

For more information, refer to the “Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls” section in the [Cisco Unified Border Element \(Enterprise\) Protocol-Independent Features and Setup Configuration Guide](#).

- **Audio Transcoding using Local Transcoding Interface (LTI):** Local Transcoding Interface (LTI) is an interface created to remove the requirement of SCCP client for CUBE transcoding.

For information, refer to [Cisco Unified Border Element 9.0 Local Transcoding Interface \(LTI\)](#).

- **Voice Class Codec (VCC) with or without Transcoding:** The Voice Class Codec feature supports basic and all Re-Invite based supplementary services like call-hold/resume, call forward, call transfer, where if any mid-call codec changes, CUBE inserts/removes/modifies the transcoder as needed.

Support for negotiation of an Audio Codec on each leg of a SIP-SIP call on the CUBE feature supports negotiation of an audio codec using the Voice Class Codec (VCC) infrastructure on CUBE.

VCC supports SIP-SIP calls on CUBE and allows mid-call codec change for supplementary services.

- **DNS SRV call routing/ load balancing:** This feature may be used by configuring a dial-peer target with a fully qualified domain name (FQDN) that resolves to a set of DNS SRV records. You can monitor all the SRV hosts that are part of the DNS destination using the OPTIONS Keepalive mechanism. It is therefore possible to load balance calls across all active destinations. For information, refer to [SIP Trunk Monitoring](#).

- **Multi-tenant based in listen-port:** This feature allows to configure specific global configurations for multiple tenants on SIP trunks. Listen ports are configured at the tenant level when there are no active calls on associated dial-peers. For information, refer to [Configure Multiple Trunks Using Tenants](#).

- **High-Availability:** The High Availability (HA) feature allows you to benefit from the failover capability of CUBE on active and standby routers. IPv6 flows in HA is supported. For information, refer to [Cisco Unified Border Element High Availability Configuration Guide](#).

- **SIP Binding:** The SIP Binding feature enables you to configure a source IP address for signaling packets and media packets. For more information, see [SIP Bind](#).

- **Inbound Dial Peer Matching (by URI):** The inbound dial peer matching by URI feature allows for the configuration of selecting inbound dial peers based on matching specific parts of the URI (Username, IP address, and DNS) received from a remote SIP entity. For more information, see [Matching Inbound Dial Peers by URI of Incoming SIP Calls](#).

- **Server Groups:** This feature configures a server group (group of server addresses) that can be referenced from an outbound dial peer. Server groups allow you to create simpler configurations by specifying a list of destination SIP servers for a single dial peer. For more information, see [Configuring Server Groups in Outbound Dial Peers](#).

- **Monitoring of Phantom Packets:** The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. For more information, see [Monitoring of Phantom Packets](#).

- **Call Admission Control:** The Call Admission Control feature enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For more information, see [Call Admission Control](#).

Prerequisites

- Enable Cisco Express Forwarding for IPv6.
- IPv6 calls does not support virtual routing and forwarding (VRF).

Restrictions

The following are the restrictions for CUBE features:

- Media Anti-Trombone feature doesn't support for IPv4-IPv6 interworking cases.
- SIPREC IPv6-to-IPv6 or IPv6-to-IPv4 call recording is not supported, if the recording server is configured on the IPv6 call leg.
- WebSocket forking, multi-VRF, RTCP report generation, NAT traversal using media keepalive, Interactive Connectivity Establishment (ICE) over IPv6 are not supported.

Configure SIP for IPv6

Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of `sip:userID@gateway.com`. The user ID can be either a username or an E.164 address. The gateway can be either a domain (with or without a hostname) or a specific Internet IPv4 or IPv6 address.

A SIP trunk can operate in one of three modes: SIP trunk in IPv4-only mode, SIP trunk in IPv6-only mode, and SIP trunk in dual-stack mode, which supports both IPv4 and IPv6.

Configure the Protocol Mode of the SIP Stack

Before you begin

SIP service should be shut down before configuring the protocol mode. After configuring the protocol mode as IPv6, IPv4, or dual-stack, SIP service should be reenabled.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sip-ua`
4. `protocol mode ipv4 | ipv6 | dual-stack [preference {ipv4 | ipv6}]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	sip-ua Example: Device(config)# sip-ua	Enters SIP user agent configuration mode.
Step 4	protocol mode ipv4 ipv6 dual-stack [preference {ipv4 ipv6}]} Example: Device(config-sip-ua)# protocol mode dual-stack	Configures the Cisco IOS SIP stack in dual-stack mode.

Example: Configuring the SIP Trunk

This example shows how to configure the SIP trunk to use dual-stack mode, with IPv6 as the preferred mode. The SIP service must be shut down before any changes are made to protocol mode configuration.

```
Device(config)# sip-ua
Device(config-sip-ua)# protocol mode dual-stack preference ipv6
```

RTCP Pass-Through

IPv4 and IPv6 addresses embedded within RTCP packets (for example, RTCP CNAME) are passed on to CUBE without being masked. These addresses are masked on the CUBE ASR 1000.

The CUBE ASR 1000 does not support printing of RTCP debugs.



Note RTCP is passed through by default. No configuration is required for RTCP pass-through.

Configure IPv6

In CUBE, IPv4-only and IPv6-only modes are not supported when endpoints are dual-stack. In this case, CUBE must also be configured in dual-stack mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **protocol mode {ipv4 | ipv6 | dual-stack {preference {ipv4 | ipv6}}}**
5. **end**

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	sip-ua Example: Device(config)# sip-ua	Enters SIP user-agent configuration mode.
Step 4	protocol mode {ipv4 ipv6 dual-stack {preference {ipv4 ipv6} ipv6}} Example: Device(config-sip-ua)# protocol mode ipv6	Configures the Cisco IOS SIP stack. • protocol mode dual-stack preference {ipv4 ipv6} —Sets the IP preference when the ANAT command is configured. • protocol mode {ipv4 ipv6} —Passes the IPv4 or IPv6 address in the SIP invite. • protocol mode dual-stack —Passes both the IPv4 addresses and the IPv6 addresses in the SIP invite and sets priority based on the far-end IP address.
Step 5	end Example: Device(conf-voi-serv)# end	Exits SIP user-agent configuration mode.

Configure the Source IPv6 Address of Signaling and Media Packets

Users can configure the source IPv4 or IPv6 address of signaling and media packets to a specific interface's IPv4 or IPv6 address. Thus, the address that goes out on the packet is bound to the IPv4 or IPv6 address of the interface specified with the **bind** command.

The **bind** command also can be configured with one IPv6 address to force the gateway to use the configured address when the bind interface has multiple IPv6 addresses. The bind interface should have both IPv4 and IPv6 addresses to send out ANAT.

When you do not specify a bind address or if the interface is down, the IP layer still provides the best local address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **bind {control | media | all} source interface *interface-id* [ipv6-address *ipv6-address*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice service VoIP configuration mode.
Step 4	sip Example: Device(config-voi-serv)# sip	Enters SIP configuration mode.
Step 5	bind {control media all} source interface <i>interface-id</i> [ipv6-address <i>ipv6-address</i>] Example: Device(config-serv-sip)# bind control source-interface FastEthernet 0/0	Binds the source address for signaling and media packets to the IPv6 address of a specific interface.

Example: Configuring the Source IPv6 Address of Signaling and Media Packets

```
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-serv-sip)# bind control source-interface fastEthernet 0/0
```


Configure the Session Target

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**mmoip** | **pots** | **vofr** | **voip**}
4. **destination pattern** [+ *string T*]
5. **session target** {**ipv4:** *destination-address* | **ipv6:** [*destination-address*] | **dns :** **\$s\$.** | **\$d\$.** | **\$e\$.** | **\$u\$.** | *host-name* | **enum:table -num** | **loopback:rtp** | **ras** | **sip-server**} [: *port*]

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	dial-peer voice <i>tag</i> { mmoip pots vofr voip } Example: Device(config)# dial-peer voice 29 voip	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
Step 4	destination pattern [+ <i>string T</i>] Example: Device(config-dial-peer)# destination-pattern 7777	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
Step 5	session target { ipv4: <i>destination-address</i> ipv6: [<i>destination-address</i>] dns : \$s\$. \$d\$. \$e\$. \$u\$. <i>host-name</i> enum:table -num loopback:rtp ras sip-server } [: <i>port</i>] Example: Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer.

Example: Configuring the Session Target

```
Device(config)# dial-peer voice 29 voip
```

```
Device(config-dial-peer)# destination-pattern 7777
Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A
```

Configure SIP Register Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **registrar {dns: address | ipv4: destination-address [: port] | ipv6: destination-address : port} aor-domain expires seconds [tcp tls]] type [secondary] [scheme string]**
5. **retry register retries**
6. **timers register milliseconds**

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	sip-ua Example: Device(config)# sip-ua	Enters SIP user agent configuration mode.
Step 4	registrar {dns: address ipv4: destination-address [: port] ipv6: destination-address : port} aor-domain expires seconds [tcp tls]] type [secondary] [scheme string] Example: Device(config-sip-ua)# registrar ipv6:2001:DB8::1:20F:F7FF:FE0B:2972 expires 3600 secondary	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports, IP phone virtual voice ports, and SCCP phones with an external SIP proxy or SIP registrar.
Step 5	retry register retries Example: Device(config-sip-ua)# retry register 10	Configures the total number of SIP register messages that the gateway should send.

	Command or Action	Purpose
Step 6	timers register <i>milliseconds</i> Example: Device(config-sip-ua)# timers register 500	Configures how long the SIP UA waits before sending register requests.

Example: Configuring SIP Register Support

```
Device(config)# sip-ua
Device(config-sip-ua)# registrar ipv6: 2001:DB8:0:0:8:800:200C:417A expires 3600 secondary
Device(config-sip-ua)# retry register 10
Device((config-sip-ua)# timers register 500
```

Configure IP Toll Fraud

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. ip address trusted list
5. ipv6 X:X:X:X::X
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice service VoIP configuration mode.

	Command or Action	Purpose
Step 4	ip address trusted list Example: Device(config-voi-serv)# ip address trusted list	Enters IP address trusted list configuration mode. You can add unique and multiple IP addresses for incoming VoIP (SIP) calls to a list of trusted IP addresses.
Step 5	ipv6 X:X:X:X::X Example: Device(cfg-iptrust-list)# ipv6 2001:DB8::/48	Enters IPv6 addresses for toll fraud prevention.
Step 6	end Example: Device(cfg-iptrust-list)# end	Exits trusted list configuration mode and returns to global configuration mode.



PART **III**

Call Control

- [Configure Tcl IVR Applications, on page 141](#)
- [Advanced Features for Cisco Contact Center, on page 153](#)



CHAPTER 14

Configure Tcl IVR Applications

- [Overview, on page 141](#)
- [Prerequisites, on page 145](#)
- [TCL IVR Configuration Tasks, on page 146](#)
- [Configure the Call Application for the Dial Peer, on page 146](#)
- [Configure TCL IVR on the Inbound VoIP Dial Peer, on page 148](#)
- [Verify TCL IVR Configuration, on page 150](#)
- [TCL IVR Configuration Examples, on page 152](#)

Overview

This chapter shows you how to configure Cisco Unified IP Interactive Voice Response (IVR) using the Tool Command Language (TCL) scripts. This chapter contains the following sections:

To identify the hardware platform or software image information that is associated with a feature in this chapter, use the [Feature Navigator](#) on Cisco.com to search for information about the feature or refer to the software release notes for a specific release.

IVR consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. It is possible to assign IVR applications to specific ports or invoke on the basis of DNIS. An IP public switched telephone network gateway can have several IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the various callers.

IVR systems provide information in the form of recorded messages over phone lines in response to user input in the form of spoken words, or more commonly dual tone multifrequency (DTMF) signaling. For example, when a user makes a call with a debit card, an IVR application is used to prompt the caller to enter a specific type of information, such as an account number. After playing the voice prompt, the IVR application collects the predetermined number of touch tones and then places the call to the destination phone or system.

IVR uses TCL scripts gather information and to process accounting and billing. For example, a TCL IVR script plays when a caller receives a voice-prompt instruction to enter a specific type of information, such as a Personal Identification Number (PIN). After playing the voice prompt, the TCL IVR application collects the predetermined number of touch tones and sends the collected information to an external server for user authentication and authorization.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Tcl IVR Enhancements

Since the introduction of the Cisco IVR technology, the software has undergone several enhancements. TCL IVR Version 2.0 is made up of separate components that are described individually in the sections that follow. The enhancements are as follows:

- Real Time Streaming Protocol (RTSP) client implementation
- TCL IVR prompt playout and digit collection on IP call legs
- New TCL verbs to utilize RTSP scripting features.

The enhancements add scalability and enable the TCL IVR scripting functionality on VoIP legs. In addition, support for RTSP enables VoIP gateways to play messages from RTSP-compliant announcement servers. The addition of these enhancements also reduces the CPU load and saves memory on the gateway because no packetization is involved. Larger prompts can be played, and the use of an external audio server is allowed.



Note TCL IVR 2.0 removed the signature locking mechanism requirement.

TCL IVR Prompts Played on IP Call Legs

TCL IVR Version 2.0 scripts is configured for incoming plain old telephone service (POTS) or VoIP call legs to play announcements to the user or collect user input (digits). With TCL IVR Version 2.0 the prompts is triggered from both the PSTN side of the call leg and the IP side of the call leg. This feature enables the audio files (or prompts) to be played out over the IP network.

TCL IVR scripts played toward a VoIP call leg are subject to the following conditions:

- G.711 mu-law encoding must be used when prompts are played.
- G.711 mu-law encoding must also be used while these calls, even at prompt playout has completed.
- Digital Signaling Protocols (DSPs) cannot be on the IP call leg so the script cannot initiate a tone.
- When a TCL IVR script is used to collect digits on a VoIP call leg, use Cisco proprietary RTP for SIP protocol configured on the call leg.



Note For additional information about the **dtmf-relay** command, refer to the [Cisco IOS Voice Command Reference - D through I](#).

IVR 2.0 enables the system to accept calls that are initiated from the IP side of the network using G.711, and terminate calls to the terminating gateway using the same codec. IP phones can also originate a call to a CUBE running an TCL IVR script.

TCL Verbs

TCL IVR, Version 2.0, delivers a new set of TCL verbs and scripts that replace the previous TCL version. The TCL verbs enable the user to develop TCL scripts that interact with the IVR application.

TCL IVR Version 2.0 is not backward compatible with the IVR 1.0 scripts.

TCL IVR scripts use the TCL verbs to interact with the gateway during call processing in order to collect the required digits—for example, to request the PIN or account number for the caller. The TCL scripts are the default scripts for all Cisco Voice features using IVR. TCL scripts are configured to control calls coming into or going out of the gateway.



Note Ensure that you have loaded the version of TCL scripts that support IVR Version 2.

The TCL IVR scripts that are shown below are listed as an example of the types of scripts available to be downloaded from the Cisco.com Software Center. For a complete list of scripts, it is recommended that you check the Software Center.

Cisco provides the following IVR scripts:

- `fax_hop_on_1`—Collects digits from the redialer, such as account number and destination number.
- `clid_authen`—Authenticates the call with Automatic Number Identification (ANI) and DNIS numbers, collects the destination data, and makes the call.
- `clid_authen_npw`—Performs as `clid_authen`, but uses a null password when authenticating, rather than DNIS numbers.
- `clid_authen_collect`—Authenticates the call with ANI and DNIS numbers and collects the destination data. If authentication fails, it collects the account and password.
- `clid_authen_col_npw`—Performs as `clid_authen_collect`, but uses a null password and does not use or collect DNIS numbers.
- `clid_col_npw_3`—Performs as `clid_authen_col_npw` except with that script, if authentication with the digits collected (account and PIN) fails, the `clid_authen_col_npw` script just plays a failure message (`auth_failed.au`) and then hangs up. The `clid_col_npw_3` script allows two failures, then plays the retry audio file (`auth_retry.au`) and collects the account and PIN again.
- The caller can interrupt the message by entering digits for the account number, triggering the prompt to tell the caller to enter the PIN. If authentication fails the third time, the script plays the audio file `auth_fail_final.au`, and hangs up.

The following table lists the prompt audio files that are associated with the `clid_col_npw_3` script.

Table 28: `clid_col_npw_3` Script Prompt Audio Files

Audio Filename	Action
<code>flash:enter_account.au</code>	Asks the caller to enter an account number. Played as the first request.
<code>flash:auth_fail_retry.au</code>	Asks the caller to reenter the account number. Plays after two failures.

flash:enter_pin.au	Asks the caller to enter a PIN.
flash:enter_destination.au	Asks the caller to enter a destination phone number.
flash:auth_fail_final.au	Informs the caller that the account number authorization has failed three times.

The following table lists additional audio files that are associated with the `clid_col_npw_3script`.

Table 29: Additional `clid_col_npw_3` Script Audio Files

Audio Filename	Action
auth_fail_retry.au	Informs the caller that authorization failed. Prompts the caller to reenter the account number followed by the pound sign (#).
auth_fail_final.au	Informs the caller, "I'm sorry, your account number cannot be verified. Please hang up and try again."

- `clid_col_npw_npw`—Tries to authenticate by using ANI, null as the user ID, user, and user password pair. If that fails, it collects an account number and authenticates with account and null. It allows three tries for the caller to enter the account number before ending the call with the authentication failed audio file. If authentication succeeds, it plays a prompt to enter the destination number.

The following table lists the audio files that are associated with the `clid_col_npw_npw` script.

Table 30: `clid_col_npw_npw` Script Audio Files

Audio Filename	Action
flash:enter_account.au	Asks the caller to enter the account number the first time.
flash:auth_fail_retry.au	Asks the caller to reenter the account number after first two failures.
flash:enter_destination.au	Asks the caller to enter the destination phone number.
flash:auth_fail_final.au	Informs the caller that the account number authorization has failed three times.

- `clid_col_dnis_3.tcl`—Authenticates the caller ID three times. First it authenticates the caller ID with DNIS. If that is not successful, it attempts to authenticate with the caller PIN up to three times.
- `clid_col_npw_3.tcl`—Authenticates with null. If authentication is not successful, it attempts to authenticate by using the caller PIN up to 3 times.
- `clid_4digits_npw_3.tcl`—Authenticates with null. If the authentication is not successful, it attempts to authenticate with the caller PIN up to 3 times using the 14-digit account number and password entered together.
- `clid_4digits_npw_3_cli.tcl`—Authenticates the account number and PIN respectively by using ANI and null. The number of digits that are allowed for the account number and password are configurable through

the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.

- `clid_authen_col_npw_cli.tcl`—Authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.
- `clid_authen_collect_cli.tcl`—Authenticates the account number and PIN by using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.
- `clid_col_npw_3_cli.tcl`—Authenticates by using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.
- `clid_col_npw_npw_cli.tcl`—Authenticates by using ANI and null for account and PIN respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.



Note To display the contents of the TCL IVR script, use the `show call application voice` command.

Prerequisites

Before you configure your CUBE to support TCL IVR, you must perform the following prerequisite tasks:

- Configure VoIP to support SIP—meaning that in addition to the basic configuration tasks, such as configuring dial peers and voice ports, you must configure specific devices in your network to act as gateways.
- Configure a TFTP sever to perform storage and retrieval of the audio files, which are required by the Debit Card gateway or other features requiring TCL IVR scripts and audio files.
- Download the appropriate TCL IVR script from the <https://d1nmyq4gcgsfi5.cloudfront.net/site/voice-gateway/downloads/sample-scripts/>. Use the `copy` command to copy your audio file (.au file) to your flash memory, and the `audio-prompt load` command to read it into RAM. When you use TCL IVR applications, the CUBE must know the URL where the TCL script can be found, and the URL of any audio file you want to use. Cisco IOS File System (IFS) is used to read the files, so any IFS-supported URLs can be used, which includes TFTP, FTP, or a pointer to a device on the router. During configuration of the application, you specify the URLs for the script and for the audio prompt. See the "Using URLs in IVR Scripts" chapter in the *TCL IVR API Version 2.0 Programmer's Guide* for more information.
- Make sure that your audio files are in the proper format. The TCL IVR prompts require audio file (.au) format of 8 bit, u-law, and 8-khz encoding.
- Install and configure the appropriate RADIUS security server in your network. The version of RADIUS that you are using must be able to support IETF-supported vendor specific attributes (VSAs), which are implemented by using IETF RADIUS attribute 26.

TCL IVR Configuration Tasks

Before starting the software configuration tasks for the TCL IVR Version 2.0 features, complete the following preinstallation tasks:

- Download the TCL scripts and audio files to be used with this feature from the <https://d1nmyq4gcgsfi5.cloudfront.net/site/voice-gateway/downloads/sample-scripts/>.
- Store the TCL scripts and audio files on a TFTP server that is accessible by CUBE.
- Create the TCL IVR application script to use with the **call application voice** command when configuring IVR using TCL scripts. You create this application first and store it on a server or location for the easy retrieval.
- Define the call flow and pass the defined parameter values to the application. Depending on the TCL script you select, these values can include the language of the audio file and the location of the audio file. [Table 28: clid_col_npw_3 Script Prompt Audio Files, on page 143](#) Lists the TCL scripts and the parameter values they require.
- Associate the application to the incoming VoIP dial peer.

Configure the Call Application for the Dial Peer

Before you begin

You must configure the application that interacts with the dial peer before you configure the dial peer. The dial peer collects digits from the caller and uses the application that you have created. Use the call application voice command as shown in the table that follows. Each command line is optional depending on the type of action that is desired or the digits to be collected.

To configure the application, enter the following commands in global configuration mode:

SUMMARY STEPS

1. **call application voice** *name url*
2. **call application voice** *name language digit language*
3. **call application voice** *name pin-length number*
4. **call application voice** *name retry-count number*
5. **call application voice** *name uid-length number*
6. **call application voice** *name set-location language category location*

DETAILED STEPS

	Command or Action	Purpose
Step 1	call application voice <i>name url</i> Example: Router(config)# call application voice <i>name url</i>	Defines the name of the application to be used with your TCL IVR script. The <i>url</i> argument specifies the location of the file and the access protocol. An example is as follows: flash:scripts/session.tcl

	Command or Action	Purpose
		<pre>tftp://dir/sarvi/scripts/session.tcl ftp://sarvi-ultra/scripts/session.tcl slot0:scripts/tcl/session..tcl</pre> <p>Note You can only configure a url if the application named <i>name</i> has <i>not</i> been configured.</p>
Step 2	<p>call application voice <i>name</i> language <i>digit</i> language</p> <p>Example:</p> <pre>Router(config)# call application voice name language digit language</pre>	<p>Specifies the language that is used by the audio files. An example is: call application voice test language 1 en. The arguments are as follows:</p> <ul style="list-style-type: none"> • <i>digit</i>—Specifies zero (0) through 9. • <i>language</i>—Specifies two characters that represent a language. For example, "en" for English, "sp" for Spanish, and "ch" for Mandarin. Enter aa to represent all.
Step 3	<p>call application voice <i>name</i> pin-length <i>number</i></p> <p>Example:</p> <pre>Router(config)# call application voice name pin-length number</pre>	<p>Defines the number of characters in the PIN for the designated application. Values are from 0 through 10.</p>
Step 4	<p>call application voice <i>name</i> retry-count <i>number</i></p> <p>Example:</p> <pre>Router(config)# call application voice name retry-count number</pre>	<p>Defines the number of times a caller is permitted to reenter the PIN for the designated application. Values are from 1 through 5.</p>
Step 5	<p>call application voice <i>name</i> uid-length <i>number</i></p> <p>Example:</p> <pre>Router(config)# call application voice name uid-length number</pre>	<p>Defines the number of characters that are allowed to be entered for the user ID for the designated application. Values are from 1 through 20.</p>
Step 6	<p>call application voice <i>name</i> set-location <i>language</i> <i>category</i> <i>location</i></p> <p>Example:</p> <pre>Router(config)# call application voicenameset-locationlanguage category location</pre>	<p>Defines the location, language, and category of the audio files for the designated application. An example is: set-location en 1 tftp://server dir/audio filename.</p>

What to do next

The following table lists TCL script names and the corresponding parameters that are required for each TCL script.

Table 31: TCL Scripts and Parameters

TCL Script Name	Description—Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	Authenticates the account number and PIN using ANI and null. The allowed length of digits is configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	Authenticates the account number and PIN using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	Authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	Authenticates using ANI and null for account and PIN. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	Authenticates using ANI and null for account and PIN. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Configure TCL IVR on the Inbound VoIP Dial Peer

Before you begin

To configure the inbound VoIP dial peer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **dial-peer voice** *4401 voip*
2. **gw-accounting VOIP**
3. **aaa authentication login VOIP radius**
4. **aaa accounting connection VOIP start-stop radius**
5. **radius-server host** *ip-address auth-port number acct-port number*
6. **application** *application-name*
7. **destination-pattern** *pattern*
8. **session protocol** *sipv2*
9. **session target**
10. **dtmf-relay rtp-nte**
11. **codec** *g711ulaw*

DETAILED STEPS

	Command or Action	Purpose
Step 1	dial-peer voice <i>4401 voip</i> Example: Router(config)# dial-peer voice <i>4401 voip</i>	Enters the dial-peer configuration mode and identifies the call leg.
Step 2	gw-accounting VOIP Example: Router(config)# gw-accounting <i>h323</i>	(Optional) Enables gateway-specific VOIP accounting.
Step 3	aaa authentication login VOIP radius Example: Router(config)# aaa authentication login VOIP radius	(Optional) Defines a method list that is called VOIP where RADIUS is defined as the only method of login authentication.
Step 4	aaa accounting connection VOIP start-stop radius Example: Router(config)# aaa accounting connection VOIP start-stop radius	(Optional) Defines a method list that is called VOIP where RADIUS is used to perform connection accounting, providing start-stop records.
Step 5	radius-server host <i>ip-address auth-port number acct-port number</i> Example: Router(config)# radius-server host <i>ip-address auth-port number acct-port number</i>	Identifies the RADIUS server and the ports that will be used for authentication and accounting services.
Step 6	application <i>application-name</i> Example: Router(config-dial-peer)# application <i>application-name</i>	Specifies the name of the application and script to use.

	Command or Action	Purpose
Step 7	destination-pattern <i>pattern</i> Example: Router(config-dial-peer)# destination-pattern <i>pattern</i>	Enters the destination pattern.
Step 8	session protocol <i>sipv2</i> Example: Router(config-dial-peer)# session protocol <i>sipv2</i>	Specifies the session protocol. The default session protocol is VOIP. The <i>sipv2</i> argument enables SIP.
Step 9	session target Example: Router(config-dial-peer)# session target	Specifies the session target IP address.
Step 10	dtmf-relay rtp-nte Example: Router(config-dial-peer)# dtmf-relay rtp-nte	Specifies the DTMF relay method. The keyword rtp-nte specifies VOIP and SIP. Note If digit collection from this VoIP call leg is required, the command dtmf-relay is required. The default is no dtmf-relay .
Step 11	codec g711ulaw Example: Router(config-dial-peer)# codec g711ulaw	Specifies the voice codec. Note If the configured application is playing prompts to the VoIP call leg, the g711ulaw keyword is required.

Verify TCL IVR Configuration

Before you begin

You can verify TCL IVR configuration by performing the following tasks:

- To verify TCL IVR configuration parameters, use the show running-config command.
- To display a list of all voice applications, use the show call application summary command.
- To display a list of all voice applications, use the show call application summary command.
- To show the contents of the script configured, use the show call application voice command.
- To verify that the operational status of the dial peer, use the show dial-peer voice command.

To verify the TCL IVR configuration, perform the following steps:

Step 1 Enter the show call application voice summary command to verify that the newly created applications are listed. The example output follows

```
Router# show call application voice summary
```


Name	Description
DEFAULT	NEW::Basic app to do DID, or supply dialtone.
fax_hop_on	Script to talk to a fax redialer
clid_authen	Authenticate with (ani, dnis)
clid_authen_collect	Authenticate with (ani, dnis), collect if that fails
clid_authen_npw	Authenticate with (ani, NULL)
clid_authen_col_npw	Authenticate with (ani, NULL), collect if that fails
clid_col_npw_3	Authenticate with (ani, NULL), and 3 tries collecting
clid_col_npw_npw	Authenticate with (ani, NULL) and 3 tries without pw
SESSION	Default system session application
hotwo	tftp://hostname/scripts/nb/nb_handoffTwoLegs.tcl
hoone	tftp://hostname/scripts/nb/nb_dohandoff.tcl
hodemst	tftp://hostname/scripts/nb/nb_handoff.tcl
clid	tftp://hostname/scripts/tcl_ivr/clid_authen_collect.tcl
db102	tftp://hostname/scripts/1.02/debitcard.tcl
*hw	tftp://171.69.184.xxx/tr_hello.tcl
*hw1	tftp://san*tr_db

```
tftp://171.69.184.235/tr_debitcard.answer.tcl
```

```
TCL Script Version 2.0 supported.
```

```
TCL Script Version 1.1 supported.
```

Note In the output shown, an asterisk (*) in an application indicates that this application was not loaded successfully. Use the **show call application voice** command with the *name* argument to view information for a particular application.

Step 2 Enter the **show dial-peer voice** command with the *peer tag* argument and verify that the application that is associated with the dial peer is correct.

Step 3 Enter the **show running-config** command to display the entire configuration.



CHAPTER 15

Advanced Features for Cisco Contact Center

- [Overview, on page 153](#)
- [Feature Information Survivability.tcl Script for Contact Center, on page 153](#)
- [Restrictions, on page 154](#)

Overview

Using the survivability.tcl script, CUBE can complement the Cisco Contact Center Enterprise solution with several unique features.

- **Courtesy Call Back:** With the Cisco Voice Portal (CVP) application, a caller may request an automated callback, rather than wait in a queue for an extended period. When an agent becomes available, CVP sends a request to place a call to the original caller. When the call is answered, the agent is connected.
- **Contact Center Survivability:** If there is a failure when connecting to an agent, the script takes control of the call and redirects it to a preconfigured destination. If the call cannot be redirected, a pre-recorded announcement from a local file is played out to the caller before disconnecting the call.

Before Cisco IOS XE Cupertino 17.9.1a, these features were only available for unencrypted PSTN trunks. From Cisco IOS XE Cupertino 17.9.1a, they may also be used with encrypted (SRTP) trunks.

For more information about CCB and callback criteria, see [Configuration Guide for Cisco Unified Customer Voice Portal, Release 12.6\(1\)](#).

Feature Information Survivability.tcl Script for Contact Center

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 32: Feature Information for Courtesy Callback with SRTP

Restrictions

- SRTP passthru cannot be used with Courtesy Call Back.



PART **IV**

Call Routing

- [Configure and Troubleshoot DNS Resolution, on page 157](#)
- [Matching Inbound Dial Peers by URI of Incoming SIP Calls, on page 163](#)
- [URI-Based Dialing Enhancements, on page 169](#)
- [Multiple Pattern Support on a Voice Dial Peer, on page 183](#)
- [Outbound Dial Peer Group as an Inbound Dial-Peer Destination, on page 189](#)
- [Inbound Leg Headers for Outbound Dial-Peer Matching, on page 197](#)
- [Server Groups, on page 207](#)
- [Domain-Based Routing , on page 217](#)
- [ENUM Enhancement per Kaplan Draft RFC, on page 225](#)



CHAPTER 16

Configure and Troubleshoot DNS Resolution

- [Overview, on page 157](#)
- [Feature Information, on page 157](#)
- [DNS Record Type, on page 158](#)
- [Select the SRV Format Version, on page 158](#)
- [Load Balance Among SRV Records, on page 159](#)
- [Configure SRV Records, on page 160](#)
- [Configure A and AAAA Records, on page 160](#)
- [DNS Queries with VRF Configuration, on page 160](#)
- [Verify the DNS Configuration on CUBE, on page 161](#)
- [Troubleshoot DNS Configuration, on page 161](#)

Overview

The Domain Name System (DNS) is a distributed database in which you can map hostnames to IP addresses through the DNS protocol from a DNS server. Each unique IP address can have an associated hostname. The conversion from a hostname to an IP address is required when hostnames are used as target endpoints under the dial-peers of the CUBE to route the calls out.

This section describes how a DNS lookup takes place in CUBE to determine the IP address that corresponds to the hostnames used for Session Initiation Protocol (SIP) calls.

Feature Information

The following table provides release information about the feature or features that are 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 software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Table 33: Feature Information for Configure and Troubleshoot DNS Lookup on CUBE on the CUBE

Feature Name	Releases	Feature Information
Configure and Troubleshoot DNS Resolution	Cisco IOS XE Cupertino 17.8.1a	Describes how Domain Name System (DNS) lookup takes place in CUBE to determine the IP address that corresponds to the hostnames used for Session Initiation Protocol (SIP) calls.

DNS Record Type

CUBE can resolve the following DNS record types:

- Service Record: SRV record is a specification of data in the DNS that defines the hostname and port number of servers for specified services. The SRV Resource Record (RR) allows you to use several servers for a single domain to move services from host to host. The SRV RR also allows you to designate some hosts as primary servers and others as backups for a service.
- Address Record (A Record): Maps a 32-bit IPv4 address to a Fully Qualified Domain Name (FQDN).
- IPv6 Address Record (AAAA) Record: Maps a 128-bit IPv6 address to an FQDN.

Select the SRV Format Version

CUBE resolves SRV records in compliance with RFC2782 by default. In this case, protocol labels are prefixed with an underscore, for example "_sip._udp.example.com". To accommodate older systems, where the underscore is not used, CUBE may be configured to use SRV version 1.

SIP RFC 2782 Compliance with DNS SRV Queries

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses the DNS SRV query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style originated in RFC 2052. Beginning with Cisco IOS XE Release 2.5, a second style, in compliance with RFC 2782, prepends the protocol label with an underscore "_"; for example, "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style.



Note The DNS SRV lookup is always attempted first for a Fully Qualified Domain Name (FQDN). If the DNS SRV lookup fails CUBE falls back to A-AAAA lookup. If you manually add a port number to an FQDN, the CUBE performs an A-AAAA lookup instead of the SRV lookup.

Example:

'session target dns: cisco.com' would perform an SRV lookup and 'session target dns:cisco.com:5060' performs an A-AAAA lookup.

To change the SRV format version, perform the following:



Note You do not have to perform this task if you want to use the default RFC 2782 format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **sip-ua**
5. **srv version** {1|2}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface gigabitethernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	sip-ua	
Step 5	srv version {1 2}	Configures the SRV version. The default version is 'srv version 2'.
Step 6	exit	

Load Balance Among SRV Records

This section lists precedence order of the records among multiple SRV entries for the same domain name.

The SRV records follow the following format:

```
_service._proto.name TTL class type of record priority weight port target
```

for example:

```
_sip._tcp.example.com 86400 IN SRV 10 60 5060 bigbox.example.com
```

```
_sip._tcp.example.com 86400 IN SRV 10 20 5060 smallbox1.example.com
_sip._tcp.example.com 86400 IN SRV 10 20 5060 smallbox2.example.com
_sip._tcp.example.com 86400 IN SRV 20 0 5060 backupbox.example.com
```

The priority field in the preceding example determines the precedence of the record's data use. Clients must use the SRV records with the lowest priority value first, and fallback to the records of higher value if the connection fails. If a service has multiple SRV records with the same priority value, the clients must load balance them in proportion to the values of their weight fields.

The first three records share a priority of 10, so the weight field's value is used by clients to determine which server (host and port combination) to contact. The sum of all three values is 100, so `bigbox.example.com` is used 60 percent of time. The two hosts, `smallbox1` and `smallbox2` are used for 40 percent of requests total, with half of them sent to `smallbox1` and the other half to `smallbox2`. If `bigbox` is unavailable, these two machines share the load equally since each is selected 50 percent of the time.

If all the three servers with priority 10 are unavailable, the record with the next lowest priority value is chosen that is `backupbox.example.com`.

Configure SRV Records

The following example shows how to configure SRV resource records that can be resolved locally for CUBE session targets:

```
ip host _sip._udp.cmgroup1.lab.local srv 1 50 5060 cucm1.lab.local
ip host _sip._udp.cmgroup1.lab.local srv 1 50 5060 cucm2.lab.local
ip host _sip._udp.cmgroup1.lab.local srv 1 50 5060 cucm3.lab.local
```



Note A or AAAA records must be configured for each SRV resource record. Refer to the "**A and AAAA records on CUBE**" section for details.

Configure A and AAAA Records

The following is the command syntax to configure A and AAAA records:

```
ip host <domain_name> <IPv4/IPv6 Address of the corresponding domain name>
```

The following are some A record examples:

```
ip host cucm1.lab.local 10.0.0.1
ip host cucm2.lab.local 10.0.0.2
ip host cucm3.lab.local 10.0.0.3
ip host cucm3.lab.local ipv6:2001:DB8:0:0:8:800:200C:417A
```

DNS Queries with VRF Configuration

While processing a SIP call, if a hostname has to be resolved, only the VRF associated with the SIP call is used during DNS resolutions. Refer to [VRF Aware DNS for SIP Calls, on page 720](#) for details.

Verify the DNS Configuration on CUBE

The following show commands are used to verify the DNS configuration on CUBE:

- **show hosts:** Displays the default domain name, the style of name lookup service, a list of name server hosts and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

```
ISR4321#show hosts
Default domain is lab.cisco.com
Name servers are 10.106.108.170
```

NAME	TTL	CLASS	TYPE	Priority	Weight	Port	DATA/ADDRESS
_sip._udp.cmgroup1.lab.local	10	IN	SRV	1	50	5060	cucm3.lab.local
_sip._udp.cmgroup1.lab.local	10	IN	SRV	1	50	5060	cucm2.lab.local
_sip._udp.cmgroup1.lab.local	10	IN	SRV	1	50	5060	cucm1.lab.local

- **show ip dns servers:** Displays the details about the list of DNS servers that are configured on CUBE.

```
ISR4321#show ip dns servers
```

IP	VRF	TTL(s)	RTT(ms)	RTO(ms)	EDNS	DNSSEC	RECURSION
10.106.108.170		791	1000	64000	Yes	Yes	Yes

- **show ip dns view:** Displays the information about a particular DNS view or about all configured DNS views. It includes the number of DNS views with details like a default domain name, list of name server hosts, and so on.

```
ISR4321#show ip dns view
DNS View default parameters:
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: lab.cisco.com
  Domain search list:
  Domain name-servers:
    10.106.108.170
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
```

Troubleshoot DNS Configuration

Use the following commands to troubleshoot DNS:

- **debug ccsip info**
- **debug ip domain detail all**
- **debug ip dns view**
- **debug ip dns view-list**
- **debug ip dns name-list**

- `debug ip domain detail all`
- `debug ip udp`



CHAPTER 17

Matching Inbound Dial Peers by URI of Incoming SIP Calls

- [Inbound Dial Peer Matching \(by URI\), on page 163](#)
- [Configure an Inbound Dial Peer to Match on URI, on page 164](#)
- [Examples for Configuring an Inbound Dial Peer to Match on a URI, on page 166](#)

Inbound Dial Peer Matching (by URI)

The inbound dial peer matching by URI feature allows you to configure the selection of inbound dial peers by matching parts of the URI sent by a remote (neighboring) SIP entity. The match is done on different parts of the URI like username, IP address, and DNS. This feature configures configuration policies, enforces specific call-treatment, security, and routing policies on each SIP trunk by originating SIP entity.

In a scenario where multiple SIP hops are involved in a call, there would be multiple via headers that are involved, and the topmost via header of an incoming SIP invite represents the last hop that forwarded the SIP request, and the bottom-most via header would represent the originator of the SIP request. This feature supports matching by the last hop that forwarded the request (neighboring SIP entity), which is the topmost via header.



Note For incoming dial-peer match based on URI, if there are multiple dial-peers matches, then the longest matching dial-peer is chosen (similar to multiple dial-peers match based on an incoming called number). However for the URI pattern match, there is no match length and hence this is the least preferred.

Feature Information

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
Inbound Dial-peer Match Based on Remote IP Address on SIP Trunks	Baseline Functionality	This feature was implemented on the Cisco Unified Border Element. The following commands were introduced or modified: dial-peer voice , voice-class uri .

Configure an Inbound Dial Peer to Match on URI

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class uri** *voice-class-uri-tag*
4. Specify a URI field for the voice class:
 - **host** *hostname-pattern*
 - **host ipv4:** *ipv4-address*
 - **host ipv6:** *ipv6-address*
 - **host dns:** *dns-address*
 - **pattern** *uri-pattern*
 - **user-id** *username-pattern*
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **session protocol sipv2**
8. **incoming uri** { **from** | **request** | **to** | **via** } *voice-class-uri-tag*
9. **end**

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	voice class uri <i>voice-class-uri-tag</i> Example:	Creates voice class for matching SIP dial peers and enters a voice URI class configuration mode.

	Command or Action	Purpose
	Device(config)# voice class uri 200	
Step 4	<p>Specify a URI field for the voice class:</p> <ul style="list-style-type: none"> • host <i>hostname-pattern</i> • host ipv4: <i>ipv4-address</i> • host ipv6: <i>ipv6-address</i> • host dns: <i>dns-address</i> • pattern <i>uri-pattern</i> • user-id <i>username-pattern</i> <p>Example:</p> <pre>Device(config-voice-uri-class)# host server1</pre> <p>Example:</p> <pre>Device(config-voice-uri-class)# host ipv4:10.0.0.0</pre> <p>Example:</p> <pre>Device(config-voice-uri-class)# host dns:xxx.yyy.com</pre>	<ul style="list-style-type: none"> • You can specify up to ten instances of the host ipv4:, host ipv6:, and host dns: commands. • You can specify only one instance of the host <i>hostname-pattern</i> commands. • Length of <i>uri-pattern</i>, <i>username-pattern</i>, and <i>hostname-pattern</i> must be less than 32. • <i>username-pattern</i> is matched against the username field of the URI. • <i>hostname-pattern</i> is matched against the host field of the URI. • <i>uri-pattern</i> is matched against the entire URI. • Only one instance of the pattern and host commands is possible. <p>Note Patterns are case-sensitive.</p>
Step 5	<p>exit</p> <p>Example:</p> <pre>Device(config-voice-uri-class)# exit</pre>	Enters global configuration mode.
Step 6	<p>dial-peer voice tag voip</p> <p>Example:</p> <pre>Device(config)# dial-peer voice 6000 voip</pre>	Enters dial peer voice configuration mode.
Step 7	<p>session protocol sipv2</p> <p>Example:</p> <pre>Device(config-dial-peer)# session protocol sipv2</pre>	Configures SIP as the session protocol type.
Step 8	<p>incoming uri { from request to via } voice-class-uri-tag</p> <p>Example:</p> <pre>Device(config-dial-peer)# incoming uri via 200</pre>	Configures the voice class with an inbound dial peer, so that it matches against configured URI fields.
Step 9	<p>end</p> <p>Example:</p> <pre>Device(config-dial-peer)# end</pre>	Exits dial peer voice configuration mode and enters privileged EXEC mode.

Examples for Configuring an Inbound Dial Peer to Match on a URI

Matching Against IPv4 Address and VIA

CUBE is configured to use incoming dial-peer 101 for incoming SIP calls from remote SIP endpoint having an IP address of 10.10.10.1

```
voice class uri 201 sip
host ipv4:10.10.10.1

dial-peer voice 101 voip
session protocol sipv2
incoming uri via 201
```

Incoming INVITE that can be matched against this dial peer.

```
INVITE sip:123@1.2.3.4:5060 SIP/2.0
Via: SIP/2.0/TCP 10.10.10.1:5093;branch=z9hG4bK-17716-1-0
Via: SIP/2.0/TCP 10.10.14.20:5093;branch=z9hG4bK-28280-1-0
```

Matching Against DNS Name and VIA

CUBE is configured to use incoming dial-peer 102 for incoming SIP calls from sample.com or an IP address that represents one of the resolved IP address of sample.com.

```
voice class uri 202 sip
host dns:sample.com

dial-peer voice 101 voip
session protocol sipv2
incoming uri via 202
```

Incoming INVITE that can be matched against this dial peer.

```
INVITE sip:123@1.2.3.4:5060 SIP/2.0
Via: SIP/2.0/TCP sample.com;branch=z9hG4bK-17716-1-0

INVITE sip:123@1.2.3.4:5060 SIP/2.0
Via: SIP/2.0/TCP 10.10.10.25:5093;branch=z9hG4bK-17716-1-0
```

10.10.10.25 is a resolved IP address of sample.com.

Matching Against Multiple Attributes and VIA

CUBE is configured to use incoming dial-peer 103 for incoming SIP calls from xxx.yyy.com, abc.def.com and IP addresses 10.10.10.10, 10.9.10.11 and 10.10.10.10.

```
voice class uri 203 sip
host dns:xxx.yyy.com
host dns:abc.def.com
host ipv4:10.10.10.10
host ipv4:10.9.10.11
host ipv4:10.10.10.10

dial-peer voice 103 voip
```



```
session protocol sipv2
incoming uri via 203
```

Incoming INVITE that can be matched against this dial peer.

```
INVITE sip:123@1.2.3.4:5060 SIP/2.0
Via: SIP/2.0/TCP 10.10.10.10:5093;branch=z9hG4bK-17716-1-0
Via: SIP/2.0/TCP 10.10.14.20:5093;branch=z9hG4bK-28280-1-0
```

10.10.10.25 is a resolved IP address of sample.com.



CHAPTER 18

URI-Based Dialing Enhancements

- [Overview, on page 169](#)
- [Configure URI Dialing, on page 173](#)
- [Example: Deriving Session Target from URI, on page 180](#)
- [Additional References for URI-Based Dialing Enhancements, on page 181](#)

Overview

The URI Dialing feature describes the enhancements that are made to Uniform Resource Identifier (URI)-based dialing on Cisco Unified Border Element (CUBE) for Session Initiation Protocol (SIP) calls. The URI-Based Dialing Enhancements feature includes support for call routing on CUBE when the User Part of the incoming Request-URI is non-E164 (for example, INVITE sip:user@abc.com).

Cisco Unified Communications Manager supports dialing using directory Uniform Resource Identifiers (URIs) for call addressing. Directory URIs follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. Use a directory URI to identify a directory number. Assign that directory number to a phone, so that Unified Communications Manager can route calls to that phone using the directory URI. URI dialing is available for Session Initiation Protocol (SIP) and Signaling Connection Control Part (SCCP) endpoints that support directory URIs.

The URI Dialing feature extends support for CUBE URI routing of calls. With these enhancements CUBE supports:

- URI routing when the User Part of the incoming Request-URI is non-E164 (for example, INVITE sip:user@abc.com).
- URI routing when the User Part is not present. The User Part is an optional parameter in the URI (for example, INVITE sip: abc.com).
- Copying the outgoing Request-URI and To header from the inbound Request-URI and To header respectively.
- Deriving (optionally) the session target for the outbound dial peer from the host portion of the inbound URI.
- URI routing for 302, Refer, and Bye Also scenarios.
- Call hunting where the subsequent dial peer is selected based on URI.
- Pass through of 302, with the host part of Contact: unmodified.



Note The minimum supported release of Cisco IOS required for URI-based call routing on dial-peers is Cisco IOS XE Gibraltar Release 16.12. You must configure the 'call-route-url' on the outgoing dial-peers to properly route the refer-to headers based on the URI matching.

Feature Information

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.

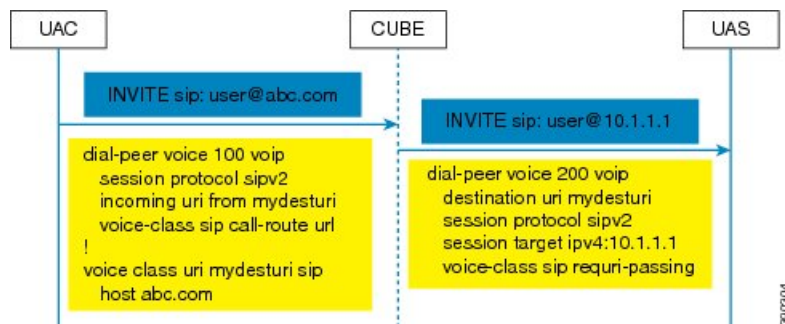
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 34: Feature Information for URI-Based Dialing Enhancements

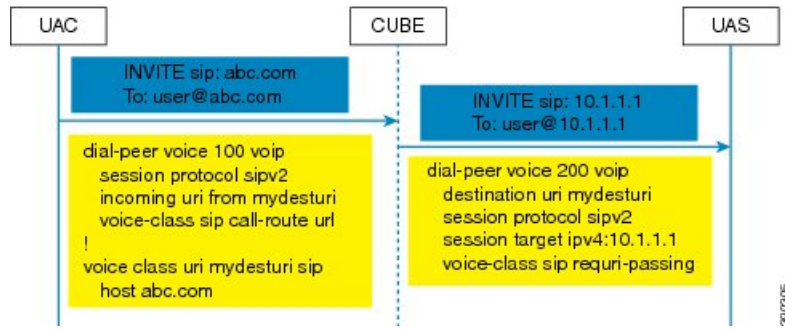
Feature Name	Releases	Feature Information
URI-Based Dialing Enhancements		The following commands were introduced or modified: contact-passing , requiri-passing , session target sip-uri and voice-class sip requiri-passing

Call Flows for URI-Based Dialing Enhancements

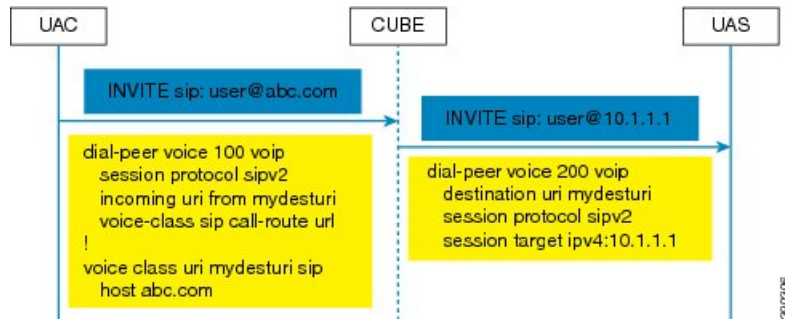
Case1: URI dialing with username being E164 or non-E164 number and Request-URI host copied from the inbound leg.



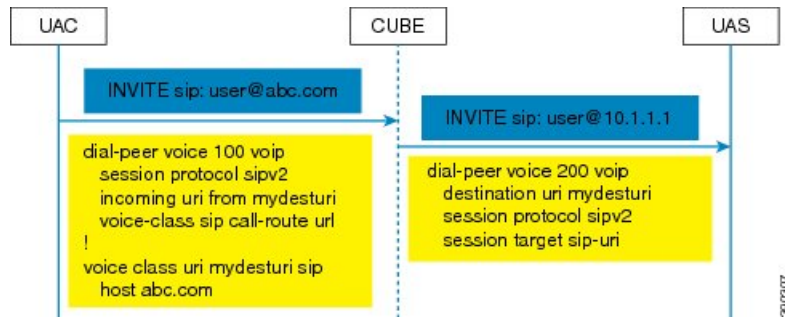
Case 2: Incoming Request-URI does not contain user part. The To: header information is also copied from the peer leg when the **requiri-passing** command is enabled.



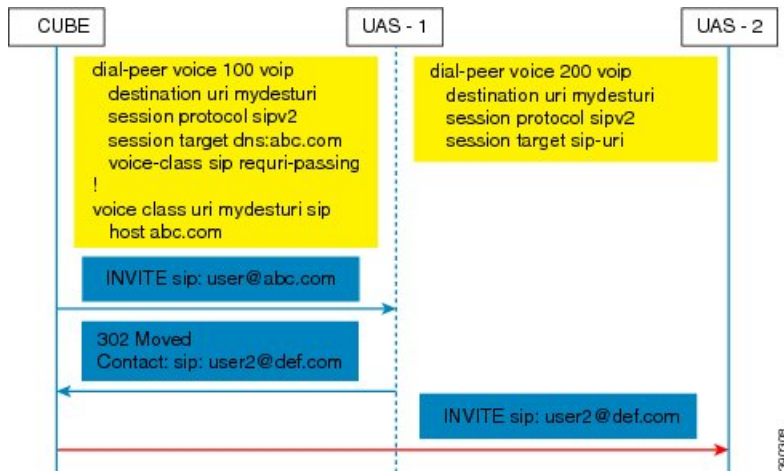
Case 3: The old behavior of setting the outbound Request-URI to session target is retained when the **requiri-passing** command is not enabled.



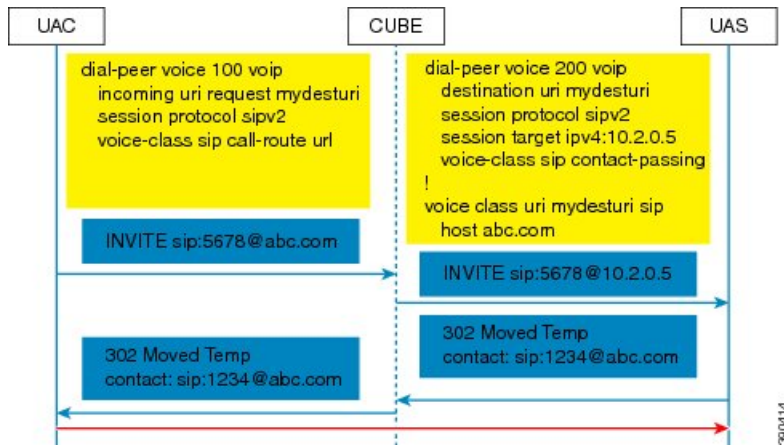
Case 4: The session target derived from the host part of the URI. The outgoing INVITE is sent to resolved IP address of the host part of the URI.



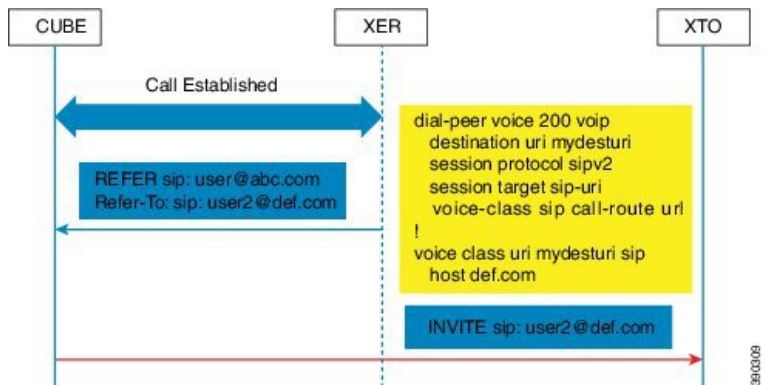
Case 5: Pass through of contact URI to request URI.



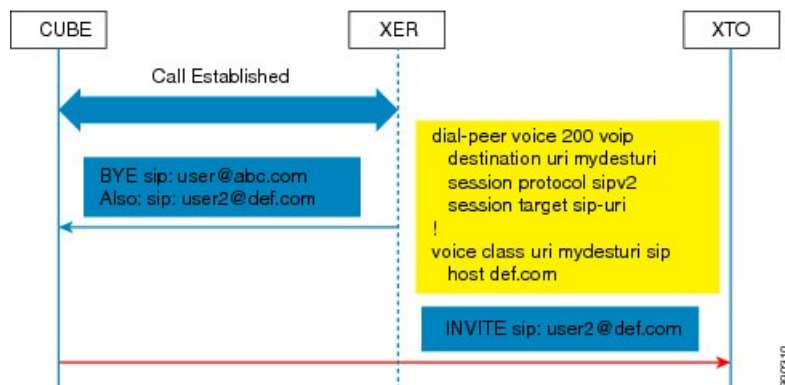
Case 6: In 302 pass-through, contact header can be passed through from one leg to another by using the **contact-passing** command.



Case 7: Pass through of refer-to URI to request URI.



Case 8: URI routing based on BYE Also header.



38/0310

Configure URI Dialing

Configure Pass Through of SIP URI Headers

Perform these tasks to configure the pass through of the host part of the Request-Uniform Resource Identifier (URI) and To Session Initiation Protocol (SIP) headers. By default, CUBE sets the host part of the URI to the value configured under the session target of the outbound dial peer. For more information, see Case 1 in the "Call Flows for URI Dialing" section.

Configure Pass Though of Request URI and To Header URI (Global Level)

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. requri-passing
6. end

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	voice service voip Example:	Specifies VoIP encapsulation and enters voice service configuration mode.

	Command or Action	Purpose
	<code>Device(config)# voice service voip</code>	
Step 4	sip Example: <code>Device(conf-voi-serv)# sip</code>	Enters the Session Initiation Protocol (SIP) configuration mode.
Step 5	requiri-passing Example: <code>Router(conf-serv-sip)# requiri-passing</code>	Enables pass through of the host part of the Request-URI and To SIP headers. By default, CUBE sets the host part of the URI to the value configured under the session target of the outbound dial peer.
Step 6	end Example: <code>Router(conf-serv-sip)# end</code>	Ends the current configuration session and returns to privileged EXEC mode.

Configure Pass Through of Request URI and to Header URI (Dial Peer Level)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class uri tag sip**
4. **host hostname-pattern**
5. **exit**
6. **dial-peer voice tag voip**
7. **session protocol sipv2**
8. **destination uri tag**
9. **session target ipv4:ip-address**
10. **voice-class sip requiri-passing [system]**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <code>Device> enable</code>	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: <code>Device# configure terminal</code>	Enters global configuration mode.
Step 3	voice class uri tag sip Example: <code>Device(config)# voice class uri mydesturi sip</code>	Creates a voice class for matching dial peers to a Session Initiation Protocol (SIP) and enters voice URI class configuration mode.

	Command or Action	Purpose
Step 4	host <i>hostname-pattern</i> Example: Device(config-voice-uri-class)# host example.com	Matches a call based on the host field in a SIP Uniform Resource Identifier (URI).
Step 5	exit Example: Device(config-voice-uri-class)# exit	Exits voice URI class configuration mode.
Step 6	dial-peer voice <i>tag voip</i> Example: Device(config)# dial-peer voice 22 voip	Defines a VoIP dial peer and enters dial peer configuration mode.
Step 7	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Specifies a session protocol for calls between local and remote routers using the Internet Engineering Task Force (IETF) SIP.
Step 8	destination uri <i>tag</i> Example: Device(config)# destination uri mydesturi	Specifies the voice class that is used to match a dial peer to the destination URI of an outgoing call.
Step 9	session target ipv4:ip-address Example: Device(config-dial-peer)# session target ipv4:10.1.1.2	Designates a network-specific address to receive calls from a VoIP.
Step 10	voice-class sip requiri-passing [system] Example: Device(config-dial-peer)# voice-class sip requiri-passing system	Enables the pass through of SIP URI headers.
Step 11	end Example: Device(config-dial-peer)# end	Ends the current configuration session and returns to privileged EXEC mode.

Configure Pass Through of 302 Contact Header

Configure Pass Through of 302 Contact Header (Global Level)

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip

5. **contact-passing**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Specifies VoIP encapsulation and enters voice service configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# sip	Enters voice service SIP configuration mode.
Step 5	contact-passing Example: Router(conf-serv-sip)# contact-passing	Enables pass through of the contact header from one leg to the other leg in 302 pass through scenario.
Step 6	end Example: Router(conf-serv-sip)# end	Ends the current configuration session and returns to privileged EXEC mode.

Configure Pass Through of 302 Contact Header (Dial Peer Level)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class uri *destination-tag* sip**
4. **user-id *id-tag***
5. **exit**
6. **voice service voip**
7. **allow-connections sip to sip**
8. **dial-peer voice *tag* voip**
9. **session protocol sipv2**
10. **destination uri *destination-tag***
11. **voice-class sip contact-passing**

12. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class uri destination-tag sip Example: Device(config)# voice class uri mydesturi sip	Creates a voice class for matching dial peers to a Session Initiation Protocol (SIP) and enters voice URI class configuration mode.
Step 4	user-id id-tag Example: Device(config-voice-uri-class)# user-id 5678	Matches a call based on the User ID portion of the Uniform Resource Identifier (URI).
Step 5	exit Example: Device(config-voice-uri-class)# exit	Exits voice URI class configuration mode.
Step 6	voice service voip Example: Device(config)# voice service voip	Specifies Voice over IP (VoIP) as the voice encapsulation type and enters voice service configuration mode.
Step 7	allow-connections sip to sip Example: Device(conf-voi-serv)# allow-connections sip to sip	Allows connections between SIP endpoints in a VoIP network.
Step 8	dial-peer voice tag voip Example: Device(config)# dial-peer voice 200 voip	Defines a VoIP dial peer and enters dial peer configuration mode.
Step 9	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Specifies a session protocol for calls between local and remote routers using the Internet Engineering Task Force (IETF) SIP.
Step 10	destination uri destination-tag Example: Device(config-dial-peer)# destination uri mydesturi	Specifies the voice class used to match a dial peer to the destination URI of an outgoing call.

	Command or Action	Purpose
Step 11	voice-class sip contact-passing Example: Device(config-dial-peer)# voice-class sip contact-passing	Enables pass through of the contact header from one leg to the other leg in 302 pass through scenario.
Step 12	end Example: Device(config-dial-peer)# end	Ends the current configuration session and returns to privileged EXEC mode.

Derive the Session Target from URI

Perform this task to derive the session target from the host part of the Uniform Resource Identifier (URI). The outgoing INVITE is sent to the resolved IP address of the host part of the URI. For more information, see Case 4 in the "Call Flows for URI-Based Dialing Enhancements" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class uri destination-tag sip**
4. **host hostname-pattern**
5. **exit**
6. **dial-peer voice tag voip**
7. **session protocol sipv2**
8. **destination uri destination-tag**
9. **session target sip-uri**
10. **exit**
11. **voice class uri source-tag sip**
12. **host hostname-pattern**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class uri destination-tag sip Example:	Creates or modifies a voice class for matching dial peers to a Session Initiation Protocol (SIP) or telephone (TEL)

	Command or Action	Purpose
	<code>Device(config)# voice class uri mydesturi sip</code>	Uniform Resource Identifier (URI) and enters voice URI class configuration mode.
Step 4	host <i>hostname-pattern</i> Example: <code>Device(config-voice-uri-class)# host destination.com</code>	Matches a call based on the host field in a SIP URI.
Step 5	exit Example: <code>Device(config-voice-uri-class)# exit</code>	Exits voice URI class configuration mode.
Step 6	dial-peer voice <i>tag voip</i> Example: <code>Device(config)# dial-peer voice 25 voip</code>	Defines a VoIP dial peer and enters dial peer configuration mode.
Step 7	session protocol <i>sipv2</i> Example: <code>Device(config-dial-peer)# session protocol sipv2</code>	Specifies a session protocol for calls between local and remote routers using the Internet Engineering Task Force (IETF) SIP.
Step 8	destination uri <i>destination-tag</i> Example: <code>Device(config-dial-peer)# destination uri mydesturi</code>	Specifies the voice class used to match a dial peer to the destination URI of an outgoing call.
Step 9	session target <i>sip-uri</i> Example: <code>Device(config-dial-peer)# session target sip-uri</code>	Derives session target from incoming URI.
Step 10	exit Example: <code>Device(config-dial-peer)# exit</code>	Exits dial peer voice configuration mode.
Step 11	voice class uri <i>source-tag sip</i> Example: <code>Device(config)# voice class uri mysourceuri sip</code>	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI and enters voice URI class configuration mode.
Step 12	host <i>hostname-pattern</i> Example: <code>Device(config-voice-uri-class)# host abc.com</code>	Matches a call based on the host field in a SIP URI.
Step 13	end Example: <code>Device(config-voice-uri-class)# end</code>	Ends the current configuration session and returns to privileged EXEC mode.

Example: Deriving Session Target from URI

```

Device> enable
Device# configure terminal
Device(config)# voice class uri mydesturi sip
Device(config-voice-uri-class)# host destination.com
Device(config-voice-uri-class)# exit
!
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# destination uri mydesturi
Device(config-dial-peer)# session target sip-uri
Device(config-dial-peer)# exit
!
Device(config)# voice class uri mysourceuri sip
Device(config-voice-uri-class)# host abc.com
Device(config-voice-uri-class)# end

```

Example: Configuring Pass Through of Request URI and To Header URI

Example: Configuring Pass Through of Request URI and To Header URI (Global Level)

```

Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# requiri-passing
Device(conf-serv-sip)# end

```

Example: Configuring Pass Through of Request URI and To Header URI (Dial Peer Level)

```

! Configuring URI voice class destination
Device(config)# voice class uri mydesturi sip
Device(config-voice-uri-class)# host xyz.com
Device(config-voice-uri-class)# exit

! Configuring outbound dial peer
Device(config)# dial-peer voice 13 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# destination uri mydesturi
Device(config-dial-peer)# session target ipv4:10.1.1.1
Device(config-dial-peer)# voice-class sip requiri-passing system
Device(config-dial-peer)# end

```

Example: Configuring Pass Through of 302 Contact Header

Example: Configuring Pass Through of 302 Contact Header (Global Level)

```

Device> enable
Device# configure terminal

```

```
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# contact-passing
Device(conf-serv-sip)# end
```

Example: Configuring Pass Through of 302 Contact Header (Dial Peer Level)

```
! Configuring URI voice class destination
Device> enable
Device# configure terminal
Device(config)# voice class uri mydesturi sip
Device(config-voice-uri-class)# user-id 5678
Device(config-voice-uri-class)# exit

! Configuring outbound dial peer
Device(config)# voice service voip
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# dial-peer voice 200 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# destination uri mydesturi
Device(config-dial-peer)# voice-class sip contact-passing
Device(config-dial-peer)# end
```

Configuration Examples for URI-Based Dialing Enhancements

Example: Deriving Session Target from URI

```
Device> enable
Device# configure terminal
Device(config)# voice class uri mydesturi sip
Device(config-voice-uri-class)# host destination.com
Device(config-voice-uri-class)# exit
!
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# destination uri mydesturi
Device(config-dial-peer)# session target sip-uri
Device(config-dial-peer)# exit
!
Device(config)# voice class uri mysourceuri sip
Device(config-voice-uri-class)# host abc.com
Device(config-voice-uri-class)# end
```

Additional References for URI-Based Dialing Enhancements

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS commands	Cisco IOS Command List, All Releases

Related Topic	Document Title
SIP configuration tasks	SIP Configuration Guide, Cisco IOS Release 15M&T

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



CHAPTER 19

Multiple Pattern Support on a Voice Dial Peer

- [Overview, on page 183](#)
- [Restrictions for Multiple Pattern Support on a Voice Dial Peer, on page 184](#)
- [Configure Multiple Pattern Support , on page 184](#)
- [Verify Multiple Pattern Support , on page 186](#)
- [Configuration Examples for Multiple Pattern Support , on page 187](#)

Overview

The Multiple Pattern Support on a Voice Dial Peer feature enables you to configure multiple patterns on a VoIP dial peer using an E.164 pattern map. A dial peer can be configured to match multiple patterns to an incoming calling or called number or an outgoing destination number.

Matching an incoming or outgoing call using a pattern defined in a VoIP dial peer is an existing feature on the Cisco Unified Border Element (Enterprise) and Session Initiation Protocol (SIP) Gateway. You can now support multiple patterns on a VoIP dial peer using an E.164 pattern map. You can create an E.164 pattern map and then link it to one or more VoIP dial peers.

When a pattern is the only source to enable a dial peer, a valid E.164 pattern map enables the linked dial peers, whereas an invalid E.164 pattern map disables the linked dial peers. Additionally, whenever an E.164 pattern map is created or reloaded, one or more dial peers linked with an E.164 pattern map is enabled or disabled based on the validation of a pattern map.

You can match a pattern map to an incoming calling or called number or an outgoing destination number.

When a dial peer has multiple patterns, the pattern with the longest prefix is considered as the matching criteria.

Feature Information for Multiple Pattern Support on a Voice Dial Peer

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 35: Feature Information for Multiple Pattern Support on a Voice Dial Peer

Feature Name	Releases	Feature Information
Configuring Multiple Pattern Support on a Voice Dial Peer (Inbound Calls)	Cisco IOS 15.4 (1)T Cisco IOS XE 3.11S	This feature was extended for inbound VoIP dial peers for incoming calling and called numbers. The following commands were introduced or modified: incoming called e164-pattern-map , incoming calling e164-pattern-map
Configuring Multiple Pattern Support on a Voice Dial Peer (Outbound Calls)	Cisco IOS 15.2(4)M Cisco IOS XE 3.7S	This feature allows you to add more than one E.164 destination pattern inside a pattern map and configure that pattern map for one or more VoIP dial peers. This feature is supported for outbound peers only. The following commands were introduced or modified: destination e164-pattern-map , e164 , show voice class e164-pattern-map , url , voice class e164-pattern-map load , voice class e164-pattern-map .

Restrictions for Multiple Pattern Support on a Voice Dial Peer

- This feature is supported only on a VoIP dial peer.
- Duplicate patterns cannot be added to a pattern map.

Configure Multiple Pattern Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class e164-pattern-map** *pattern-map-id*
4. Do one of the following:
 - **e164** *pattern-map-tag*
 - **url** *url*

5. (Optional) **description** *string*
6. **exit**
7. **dial-peer voice** *dial-peer-id* **voip**
8. {**destination** | **incoming called** | **incoming calling**} **e164-pattern-map** *pattern-map-group-id*
9. **end**
10. (Optional) **voice class e164-pattern-map load** *pattern-map-group-id*
11. **show dial-peer voice** [**summary** | *dial-peer-id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class e164-pattern-map <i>pattern-map-id</i> Example: Device(config)# voice class e164-pattern-map 1111	Creates a pattern map for configuring one or multiple E.164 patterns on a dial peer and enters voice class configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> • e164 <i>pattern-map-tag</i> • url <i>url</i> Example: Using URL text file: Device(voice-class)# url http://http-host/config-files/pattern-map.cfg Directly specifying match patterns: Device(voice-class)# e164 5557123	Configure one or more E.164 telephone number prefix match patterns for the pattern map. <ul style="list-style-type: none"> • Repeat this step for each pattern if you are using the e164 command. • You can specify a file URL containing the patterns for this dial peer using the url url command. You must then load the E.164 telephone prefixes using Step 10. The file can be internal (on the device) or external.
Step 5	(Optional) description <i>string</i> Example: Device(voice-class)# description It has 1 entry	Provides a description for the pattern map.
Step 6	exit Example:	Exits voice class configuration mode and enters global configuration mode.

	Command or Action	Purpose
	Device (voice-class) # exit	
Step 7	dial-peer voice <i>dial-peer-id</i> voip Example: Device (config) # dial-peer voice 2222 voip	Defines a VoIP dial peer and enters dial peer configuration mode.
Step 8	{ destination incoming called incoming calling } e164-pattern-map <i>pattern-map-group-id</i> Example: Device (config-dial-peer) # incoming calling e164-pattern-map 1111	Links a pattern-map group with a dial peer. <ul style="list-style-type: none"> • Use the destination keyword for outbound dial peers. • Use the incoming called or incoming calling keywords for inbound dial peers using called or calling numbers.
Step 9	end Example: Device (config-dial-peer) # end	Exits dial peer configuration mode and enters privileged EXEC mode.
Step 10	(Optional) voice class e164-pattern-map load <i>pattern-map-group-id</i> Example: Device # voice class e164-pattern-map load 1111	Loads the specified pattern map with E.164 match patterns from a text file configured in the pattern map. <ul style="list-style-type: none"> • This step is required only if patterns have been defined for the specified pattern map using a file URL in Step 4.
Step 11	show dial-peer voice [summary <i>dial-peer-id</i>] Example: Device # show dial-peer voice 1111	Displays the status of a pattern map when the pattern map is associated with a dial peer.

Verify Multiple Pattern Support

SUMMARY STEPS

1. **show voice class e164-pattern-map** [**summary** | *pattern-map-id*]
2. **show dial-peer voice** [**summary** | *dial-peer-id*]
3. **show dialplan incall** {**sip** | **h323**} {**calling** | **called**} *e164-pattern*

DETAILED STEPS

Step 1 **show voice class e164-pattern-map** [**summary** | *pattern-map-id*]

Displays the status and contents of a specified pattern map or a status summary of all pattern maps.

Example:

```
Device# show voice class e164-pattern-map 200
```

```
e164-pattern-map 200
-----
It has 1 entries
It is not populated from a file.
Map is valid.

E164 pattern
-----
200
```

Step 2 `show dial-peer voice [summary | dial-peer-id]`

Displays the status of pattern maps associated with all or a specified dial peer.

Example:

```
Device# show dial-peer voice | include e164-pattern-map

    incoming calling e164-pattern-map tag = `200' status = valid,
    destination e164-pattern-map tag = 3000 status = valid,

Device# show dial-peer voice 2222 | include e164-pattern-map

    incoming calling e164-pattern-map tag = `200' status = valid,
```

Step 3 `show dialplan incall {sip | h323} {calling | called} e164-pattern`

Displays inbound dial peer details and associated pattern maps based on an incoming calling or called number.

Example:

```
Device# show dialplan incall voip calling 23456

VoiceOverIpPeer1234567
  peer type = voice, system default peer = FALSE, information type = voice,
  description = `',
  tag = 1234567, destination-pattern = `',
  destination e164-pattern-map tag = 200 status = valid,
  destination dpd tag = 200 status = valid,
  voice reg type = 0, corresponding tag = 0,
  allow watch = FALSE
  answer-address = `', preference=0,
  incoming calling e164-pattern-map tag = `200' status = valid,
  CLID Restriction = None
```

Configuration Examples for Multiple Pattern Support

Example: Configuring Multiple Patterns for Outbound Dial Peers Using a File URL

```
Device# voice class e164-pattern-map 1111
Device(voice-class)# url http://http-host/config-files/pattern-map.cfg
Device(voice-class)# description For Outbound Dial Peer
```

```
Device(voice-class)# exit
Device(config)# dial-peer voice 2222 voip
Device(voice-dial-peer)# destination e164-pattern-map 1111
Device(voice-dial-peer)# exit
Device(config)# voice class e164-pattern-map load 1111
Device(config)# end
```

Example: Configuring Multiple Patterns for Outbound Dial Peers by Specifying Each E164 Pattern

```
Device# voice class e164-pattern-map 1112
Device(voice-class)# e164 5557456
Device(voice-class)# e164 5557455
Device(voice-class)# e164 5557454
Device(voice-class)# e164 5557453
Device(voice-class)# e164 5557452
Device(voice-class)# description For Outbound Dial Peer
Device(voice-class)# exit
Device(config)# dial-peer voice 2222 voip
Device(voice-dial-peer)# destination e164-pattern-map 1112
Device(voice-dial-peer)# end
!
```

Example: Configuring Multiple Patterns for Inbound Dial Peer

```
Device# voice class e164-pattern-map 1113
Device(voice-class)# url http://http-host/config-files/pattern-map.cfg
Device(voice-class)# description For Inbound Dial Peer
Device(voice-class)# exit
Device(config)# dial-peer voice 2222 voip
Device(voice-dial-peer)# incoming calling e164-pattern-map 1113
Device(voice-dial-peer)# exit
Device(config)# voice class e164-pattern-map load 1113
Device(config)# end
```



CHAPTER 20

Outbound Dial Peer Group as an Inbound Dial-Peer Destination

- [Overview, on page 189](#)
- [Restrictions, on page 190](#)
- [Configure Outbound Dial-Peer Group as an Inbound Dial-Peer Destination, on page 190](#)
- [Verifying Outbound Dial-Peer Groups as an Inbound Dial-Peer Destination, on page 193](#)
- [Troubleshooting Tips, on page 194](#)
- [Configuration Examples for Outbound Dial Peer Group as an Inbound Dial-Peer Destination, on page 195](#)

Overview

This feature can group multiple outbound dial peers into a dial-peer group and configure this dial-peer group as the destination of an inbound dial peer.

You can group up to 20 outbound (SIP) dial peers into a dial-peer group and configure this dial-peer group as the destination of an inbound dial peer. Once an incoming call is matched by an inbound dial peer with an active destination dial-peer group, dial peers from this group are used to route the incoming call. No other outbound dial-peer provisioning to select outbound dial peers is used.

A preference can be defined for each dial peer in a dial-peer group. This preference is used to decide the order of selection of dial peers from the group for the setup of an outgoing call.

You can also specify various dial-peer hunt mechanism using the existing **dial-peer hunt** command.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 36: Feature Information

Feature Name	Releases	Feature Information
Support for POTS dial-peer	Baseline Functionality	An outgoing POTS dial peer can be part of a dial-peer group. An inbound POTS dial peer can have a dial-peer group as the destination.

Restrictions

- If a dial-peer group is in the shutdown state, regular dial-peer search occurs.
- If all dial-peers in an active dial-peer group are unavailable, call is disconnected.
- Calls are statically routed to one of the dial-peers in the active dial-peer group.
- The **destination-pattern** command is required on the outbound dial-peer even though matching is not done based on this command.
- The outgoing call setup is deferred until inter-digit timer expires or a terminator is entered.
- Dial-peer group works only with valid E.164 pattern.

For POTS dial-peers:

- Two-stage dialing is not supported.
- Overlapping dialing is not supported.
- TCL and VXML routing changes are not supported.
- Digit-stripping is not supported.

Configure Outbound Dial-Peer Group as an Inbound Dial-Peer Destination

Perform this task to configure a dial-peer group with multiple outbound peers and an inbound dial peer referencing this dial-peer group as a destination.

Before you begin

- Configure SIP outbound dial peers to be associated with a dial-peer group.
- For an outbound POTS dial peer, ensure that **destination-pattern .T** and **no digit-strip** are configured to avoid unexpected dialed digit strip.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *outbound-dial-peer-id* [**voip** | **pots**]
4. **destination-pattern** *pattern*
5. **no digit-strip** for POTS dial peers.
6. **exit**
7. (Optional) **dial-peer hunt** *hunt-order-number*
8. **voice class dpg** *dial-peer-group-id*
9. **dial-peer** *outbound-dial-peer-id* [**preference** *preference-order*]
10. (Optional) **description** *string*
11. **exit**
12. **dial-peer voice** *inbound-dial-peer-id* [**voip** | **pots**]
13. **destination dpg** *dial-peer-group-id*
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>outbound-dial-peer-id</i> [voip pots] Example: For VoIP dial peer: Device(config)# dial-peer voice 123 voip Example: For POTS dial peer: Device(config)# dial-peer voice 345 pots	Defines a dial peer and enters dial peer configuration mode.
Step 4	destination-pattern <i>pattern</i> Example: For VoIP Dial Peers Device(config-dial-peer)# destination-pattern 1004	Configures a destination pattern. This step is required even though the value is not used for dial-peer matching.

	Command or Action	Purpose
	<p>Example:</p> <p>For POTS Dial Peers</p> <pre>Device(config-dial-peer)# destination-pattern .T</pre>	
Step 5	<p>no digit-strip for POTS dial peers.</p> <p>Example:</p> <pre>Device(config-dial-peer)# no digit-strip</pre>	Disable unexpected dialed digit strip.
Step 6	<p>exit</p> <p>Example:</p> <pre>Device(config-dial-peer)# exit</pre>	Exits to global configuration mode.
Step 7	<p>(Optional) dial-peer hunt <i>hunt-order-number</i></p> <p>Example:</p> <pre>Device(config)# dial-peer hunt 0</pre>	<p>Specifies a hunt selection mechanism for dial peers.</p> <ul style="list-style-type: none"> The default mechanism is random selection.
Step 8	<p>voice class dpg <i>dial-peer-group-id</i></p> <p>Example:</p> <pre>Device(config)# voice class dpg 181</pre>	<p>Creates a dial-peer group for grouping multiple outbound dial peers and enters voice class configuration mode.</p> <ul style="list-style-type: none"> You can use the shutdown command to resume regular outbound dial-peer provisioning in dial-peers with this dial-peer group as destination.
Step 9	<p>dial-peer <i>outbound-dial-peer-id</i> [preference <i>preference-order</i>]</p> <p>Example:</p> <pre>Device(config-class)# dial-peer 123 preference 1</pre>	<p>Associates a configured outbound dial peer with this dial-peer group and configures a preference value.</p> <ul style="list-style-type: none"> Repeat this step for all outbound dial-peers that need to be added to this dial-peer group. If preference is not specified, the order of selection is random or as specified by the dial-peer hunt command.
Step 10	<p>(Optional) description <i>string</i></p> <p>Example:</p> <pre>Device(config-class)# description Boston Destination</pre>	Provides a description for the dial-peer group.
Step 11	<p>exit</p> <p>Example:</p> <pre>Device(config-class)# exit</pre>	Exits voice class configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 12	dial-peer voice <i>inbound-dial-peer-id</i> [voip pots] Example: For VoIP dial peer: <pre>Device(config)# dial-peer voice 789 voip</pre> Example: For POTS dial peer: <pre>Device(config)# dial-peer voice 678 pots</pre>	Defines a dial peer and enters dial peer configuration mode.
Step 13	destination dpg <i>dial-peer-group-id</i> Example: <pre>Device(config-dial-peer)# destination dpg 181</pre>	Specifies a dial peer group from which an outbound dial peer can be chosen.
Step 14	end Example: <pre>Device(config-dial-peer)# end</pre>	Exits dial peer configuration mode and enters privileged EXEC mode.

Verifying Outbound Dial-Peer Groups as an Inbound Dial-Peer Destination

SUMMARY STEPS

1. **show voice class dpg** *dial-peer-group-id*
2. **show dial-peer voice** *inbound-dial-peer-id*

DETAILED STEPS

Step 1 **show voice class dpg** *dial-peer-group-id*

Displays the configuration of an outbound dial-peer group.

Example:

```
Device# show voice class dpg 200
```

```
Voice class dpg: 200      AdminStatus: Up
Description: Boston Destination
Total dial-peer entries: 4
```

```
Peer Tag      Pref
-----      ----
1001          1
1002          2
1004          0
```

```
1003          1
-----
```

Step 2 **show dial-peer voice** *inbound-dial-peer-id*

Displays the referencing of destination dial-peer group from an inbound dial peer.

Example:

```
Device# show dial-peer voice 100 | include destination dpg
        destination dpg tag = 200 status = valid,
```

Troubleshooting Tips

SUMMARY STEPS

1. Enter the following:
 - **debug voip dialpeer inout**
 - **debug voip ccapi inout**

DETAILED STEPS

Enter the following:

- **debug voip dialpeer inout**
- **debug voip ccapi inout**

Displays the configuration of an outbound dial-peer group.

Example:

```
*Jul 19 10:15:53.310 IST: //-1/ED647BD1B0F9/DPM/dpMatchCore:
  Dial String=4001, Expanded String=4001, Calling Number=
  Timeout=TRUE, Is Incoming=TRUE, Peer Info Type=DIALPEER_INFO_SPEECH
*Jul 19 10:15:53.310 IST: //-1/xxxxxxxxxxxx/DPM/vepm_match_pattern_map:
  DEPM 1000 use caching dialstring 4001 status 0
*Jul 19 10:15:53.310 IST: //-1/ED647BD1B0F9/DPM/MatchNextPeer:
```

Incoming dial peer is first matched:

```
Result=Success(0); Incoming Dial-peer=600 Is Matched
*Jul 19 10:15:53.310 IST: //-1/ED647BD1B0F9/DPM/dpMatchPeertype:exit@6602
*Jul 19 10:15:53.310 IST: //-1/ED647BD1B0F9/DPM/dpAssociateIncomingPeerCore:
  Result=Success(0) after DP_MATCH_INCOMING_DNIS; Incoming Dial-peer=600
*Jul 19 10:15:53.310 IST: //-1/ED647BD1B0F9/DPM/dpMatchSafModulePlugin:
  dialstring=NULL, saf_enabled=0, saf_dndb_lookup=0, dp_result=0
*Jul 19 10:15:53.310 IST: //-1/ED647BD1B0F9/DPM/dpAssociateIncomingPeerSPI:exit@7181
*Jul 19 10:15:53.311 IST: //-1/ED647BD1B0F9/DPM/dpMatchPeersCore:
  Calling Number=, Called Number=4001, Peer Info Type=DIALPEER_INFO_SPEECH
```

The dial-peer group associated with a dial peer is selected:

```
*Jul 19 10:15:53.311 IST: //-1/ED647BD1B0F9/DPM/dpMatchPeersCore:
  Outbound Destination DPG Group Request; Destination DPG=1
*Jul 19 10:15:53.311 IST: //-1/ED647BD1B0F9/DPM/dpMatchDestDPGGroup:
  Result=0
*Jul 19 10:15:53.311 IST: //-1/ED647BD1B0F9/DPM/dpMatchPeersCore:
  Result=SUCCESS(0) after DestDPGGroup
*Jul 19 10:15:53.311 IST: //-1/ED647BD1B0F9/DPM/dpMatchSafModulePlugin:
  dialstring=4001, saf_enabled=0, saf_dndb_lookup=1, dp_result=0
```

List of active Dial-peers configured within the DPG, sorted by preference:

```
*Jul 19 10:15:53.311 IST: //-1/ED647BD1B0F9/DPM/dpMatchPeersMoreArg:
  Result=SUCCESS(0)
List of Matched Outgoing Dial-peer(s):
  1: Dial-peer Tag=1004
  2: Dial-peer Tag=1001
  3: Dial-peer Tag=1003
  4: Dial-peer Tag=1002
```

Configuration Examples for Outbound Dial Peer Group as an Inbound Dial-Peer Destination

```
Device> enable
Device# configure terminal
! Configuring outbound dial peers that are to be grouped.
Device(config)# dial-peer voice 1001 voip
Device(config-dial-peer)# destination-pattern 1001
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.1.1.1
Device(config-dial-peer)# exit

Device(config)# dial-peer voice 1002 voip
Device(config-dial-peer)# destination-pattern 1002
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.1.1.2
Device(config-dial-peer)# exit

Device(config)# dial-peer voice 1003 voip
Device(config-dial-peer)# destination-pattern 1003
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.1.1.3
Device(config-dial-peer)# exit

Device(config)# dial-peer voice 1004 pots
Device(config-dial-peer)# destination-pattern 5...
Device(config-dial-peer)# no digit-strip
Device(config-dial-peer)# direct-inward-dial
Device(config-dial-peer)# port 1/0/0:23
```

```

Device(config-dial-peer)# forward-digits all
Device(config-dial-peer)# exit

!Grouping outbound dial peers and configuring preferences if needed.
Device(config)# voice class dpg 200
Device(config-class)# dial-peer 1001 preference 1
Device(config-class)# dial-peer 1002 preference 2
Device(config-class)# dial-peer 1003 preference 3
Device(config-class)# dial-peer 1004 preference 4
Device(config-class)# description Boston Destination
Device(config-class)# exit

!Associating outbound dial peer group with an inbound dial peer group.
Device(config)# dial-peer voice 100 voip
Device(config-dial-peer)# incoming called-number 13411
Device(config-dial-peer)# destination dpg 200
Device(config-dial-peer)# end

!Associating outbound dial peer group with an inbound POTS dial peer group.
Device(config)# dial-peer voice 600 pots
Device(config-dial-peer)# incoming called-number 4T
Device(config-dial-peer)# destination dpg 200
Device(config-dial-peer)# end

```

Verifying Outbound Dial-Peer Group Configuration

```

Device# show voice class dpg 200

Voice class dpg: 200      AdminStatus: Up
Description: Boston Destination
Total dial-peer entries: 4

Peer Tag      Pref
-----      ----
1001          1
1002          2
1004          0
1003          1
-----

```

Verifying Inbound Dial-Peer Referencing Outbound Dial-Peer Group

```

Device# show dial-peer voice 100 | include destination dpg

destination dpg tag = 200 status = valid,
Device# show dial-peer voice 600 | include destination dpg

destination dpg tag = 200 status = valid,

```



CHAPTER 21

Inbound Leg Headers for Outbound Dial-Peer Matching

- [Overview, on page 197](#)
- [Prerequisites for Inbound Leg Headers for Outbound Dial-Peer Matching, on page 198](#)
- [Restrictions for Inbound Leg Headers for Outbound Dial-Peer Matching, on page 198](#)
- [Configuring Inbound Leg Headers for Outbound Dial-Peer Matching, on page 199](#)
- [Verify Inbound Leg Headers for Outbound Dial-Peer Matching, on page 201](#)
- [Configuration Example: Inbound Leg Headers for Outbound Dial-Peer Matching, on page 204](#)

Overview

The Inbound Leg Headers for Outbound Dial-Peer Matching feature allows you to match and provision an outbound dial peer for an outbound call leg using the headers from an inbound call leg. The following headers of an incoming call leg can be used for outbound dial-peer matching:

- VIA (SIP Header)
- FROM (SIP Header)
- TO (SIP Header)
- DIVERSION (SIP Header)
- REFERRED BY (SIP Header)
- Called Number
- Calling Number
- Carrier ID

The above headers are retrieved from an incoming INVITE or REFER message and used for outbound dial-peer provisioning.

SIP headers of an INVITE message are saved to an associated call leg. For example, an INVITE message is received for a new call leg A. Then, SIP headers are saved to call leg A itself for outbound dial-peer lookup.

On the other hand, SIP headers of a REFER message are saved to the peer call leg of the associated call leg. For example, call leg A and call leg B are connected in CUBE. The party at Call Leg B makes a blind transfer

to the party at Call Leg C. The party at Call Leg B (transferor) makes a blind transfer to the party at call leg C, triggering a SIP REFER message which the party at Call Leg B sends to CUBE for the transfer to C.

Feature Information

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 37: Feature Information for Inbound Leg Headers for Outbound Dial-PeerMatching

Feature Name	Releases	Feature Information
Inbound Leg Headers for Outbound Dial-PeerMatching	Baseline Functionality	The following commands were introduced by this feature: destination provision-policy , destination uri-via , destination uri-to , destination uri-from , destination uri-diversion , destination uri-referred-by , show voice class dial-peer provision-policy

Prerequisites for Inbound Leg Headers for Outbound Dial-PeerMatching

- CUBE or Voice Gateway must be configured.

Restrictions for Inbound Leg Headers for Outbound Dial-PeerMatching

- The existing **header-passing** command supports modification of SIP headers of INVITE message by the Tool Command Language (TCL) application. If the above SIP headers are modified by the TCL application, they cannot be used for outbound dial-peer provisioning.
- If multiple SIP via headers and diversion headers are found in an incoming INVITE or REFER message, only the top-most via header and top-most diversion header of an incoming INVITE or REFER message are used for outbound dial-peer provisioning.
- When an incoming call is matched to an inbound dial peer with an associated provision profile without rules, outbound dial-peer provisioning is disabled and the incoming call is disconnected by CUBE or voice gateway with cause code "unassigned number (1)".

Configuring Inbound Leg Headers for Outbound Dial-PeerMatching

Before you begin

Necessary pattern maps have been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class dial-peer provision-policy tag**
4. (Optional) **description string**
5. **preference preference-order first-attribute second-attribute**
6. **exit**
7. **dial-peer voice inbound-dial-peer-tag voip**
8. **destination provision-policy tag**
9. **exit**
10. **dial-peer voice outbound-dial-peer-tag voip**
11. Configure a match command for an outbound dial peer according to the provision policy rule attribute configured.
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class dial-peer provision-policy tag Example: Device(config)# voice class dial-peer provision-policy 200	Creates a provision policy profile in which a set of attributes for dial-peer matching can be defined. <ul style="list-style-type: none"> • You can use the shutdown command to deactivate the provision policy and allow normal outbound dial-peer provisioning.
Step 4	(Optional) description string Example:	Provides a description for the provision policy profile.

	Command or Action	Purpose																				
	Device(voice-class)# description match both calling and called																					
Step 5	<p>preference <i>preference-order first-attribute second-attribute</i></p> <table border="1"> <thead> <tr> <th>First Attribute</th> <th>Second Attribute</th> </tr> </thead> <tbody> <tr> <td>diversion</td> <td>from, referred-by, to, uri, via</td> </tr> <tr> <td>from</td> <td>diversion, referred-by, to, uri, via</td> </tr> <tr> <td>referred-by</td> <td>diversion, from, to, uri, via</td> </tr> <tr> <td>to</td> <td>diversion, referred-by, from, uri, via</td> </tr> <tr> <td>uri</td> <td>diversion, referred-by, to, from, via, carrier-id</td> </tr> <tr> <td>via</td> <td>diversion, referred-by, to, uri, from</td> </tr> <tr> <td>called</td> <td>calling, carrier-id</td> </tr> <tr> <td>calling</td> <td>called</td> </tr> <tr> <td>carrier-id</td> <td>called, uri</td> </tr> </tbody> </table> <p>Example:</p> <pre>Device(voice-class)# preference 2 calling called</pre>	First Attribute	Second Attribute	diversion	from, referred-by, to, uri, via	from	diversion, referred-by, to, uri, via	referred-by	diversion, from, to, uri, via	to	diversion, referred-by, from, uri, via	uri	diversion, referred-by, to, from, via, carrier-id	via	diversion, referred-by, to, uri, from	called	calling, carrier-id	calling	called	carrier-id	called, uri	<p>Configures a provision policy rule.</p> <ul style="list-style-type: none"> You can configure up to two rules. This means up to four attributes can be configured for matching outbound dial peers. If rules are not configured, outbound dial-peer provisioning is disabled, and an incoming call matched to an inbound dial peer associated with this profile is disconnected by CUBE or voice gateway with cause code "unassigned number (1)".
First Attribute	Second Attribute																					
diversion	from, referred-by, to, uri, via																					
from	diversion, referred-by, to, uri, via																					
referred-by	diversion, from, to, uri, via																					
to	diversion, referred-by, from, uri, via																					
uri	diversion, referred-by, to, from, via, carrier-id																					
via	diversion, referred-by, to, uri, from																					
called	calling, carrier-id																					
calling	called																					
carrier-id	called, uri																					
Step 6	<p>exit</p> <p>Example:</p> <pre>Device(voice-class)# exit</pre>	Exits voice class configuration mode and enters global configuration mode.																				
Step 7	dial-peer voice <i>inbound-dial-peer-tag voip</i>	Enters dial peer configuration mode for an inbound dial peer.																				
Step 8	<p>destination provision-policy <i>tag</i></p> <p>Example:</p> <pre>Device(config)# dial-peer voice 100 voip Device(config-dial-peer)# destination provision-policy 200 Device(config)# exit</pre>	Associates a provision policy profile with an inbound dial peer.																				
Step 9	exit	Exits dial peer configuration mode.																				
Step 10	dial-peer voice <i>outbound-dial-peer-tag voip</i>	Enters dial peer configuration mode for an outbound dial peer.																				

	Command or Action	Purpose	
Step 11	Configure a match command for an outbound dial peer according to the provision policy rule attribute configured.	Configure a match command based on any of the four attributes defined in the provision policy rule.	
	Provision Policy Rule Attribute		Dial-peer Match command
	called		destination-pattern <i>pattern</i> destination e164-pattern-map <i>pattern-map-class-id</i>
	calling		destination calling e164-pattern-map <i>pattern-map-class-id</i>
	carrier-id		carrier-id target
	uri		destination uri <i>uri-class-tag</i>
	via		destination uri-via <i>uri-class-tag</i>
	to		destination uri-to <i>uri-class-tag</i>
	from		destination uri-from <i>uri-class-tag</i>
	diversion		destination uri-diversion <i>uri-class-tag</i>
referred-by	destination uri-referred-by <i>uri-class-tag</i>		
	Example: Device(config)# dial-peer voice 300 voip Device(config-dial-peer)# destination uri-from 200 Device(config)# exit		
Step 12	end Example: Device(config-dial-peer)# end	Exits dial peer configuration mode and enters privileged EXEC mode.	

Verify Inbound Leg Headers for Outbound Dial-PeerMatching

Use this procedure to verify inbound leg headers so that you can match them to Outbound dial peers.

SUMMARY STEPS

1. **show dialplan incall {sip | h323} {calling | called} e164-pattern | include voice**
2. **show dialplan dialpeer inbound-dial-peer-id number e164-pattern [timeout] | include Voice**
3. **show voice class dial-peer provision-policy**

DETAILED STEPS

Step 1 **show dialplan incall {sip | h323} {calling | called} e164-pattern | include voice**

Displays inbound dial peers based on an incoming calling or called number. Once you have the dial peer number, you can use it to search for the complete dial-peer details in the running-config.

Example:

```
Device# show dialplan incall sip calling 3333 | include Voice
```

```
VoiceOverIpPeer1
```

```
Device# show dialplan incall sip calling 4444 | include Voice
```

```
VoiceOverIpPeer1
```

```
Device# show running-config | section dial-peer voice 1 voip
```

```
dial-peer voice 1 voip
 destination dpg 10000
 incoming calling e164-pattern-map 100
 dtmf-relay rtp-nte
 codec g711ulaw
```

```
Device# show dialplan incall sip called 6000 timeout | include Voice
```

```
VoiceOverIpPeer100
```

```
Device# show running-config | section dial-peer voice 100 voip
```

```
dial-peer voice 100 voip
 incoming called e164-pattern-map 1
 incoming calling e164-pattern-map 1
 dtmf-relay rtp-nte
 codec g711ulaw
```

```
Device# show dialplan incall voip calling 23456
```

```
VoiceOverIpPeer1234567
 peer type = voice, system default peer = FALSE, information type = voice,
 description = `',
 tag = 1234567, destination-pattern = `',
 destination e164-pattern-map tag = 200 status = valid,
 destination dpg tag = 200 status = valid,
 voice reg type = 0, corresponding tag = 0,
 allow watch = FALSE
 answer-address = `', preference=0,
 incoming calling e164-pattern-map tag = `200' status = valid,
 CLID Restriction = None
```

Step 2 **show dialplan dialpeer inbound-dial-peer-id number e164-pattern [timeout] | include Voice**

Displays a list of outbound dial peers based on a specified inbound dial peer. This command line will be helpful find a list of outbound dial peer of a destination dial-peer group.

Example:

```
Device# show dialplan dialpeer 1 number 23457 timeout | include Voice
```

```
VoiceOverIpPeer100013
```

```
VoiceOverIpPeer100012
```

Example:

```

voice class dial-peer provision-policy 2000
  preference 2 diversion to
!
...
!
dial-peer voice 32555 voip
  session protocol sipv2
  session target ipv4:1.5.14.9
  destination uri-diversion 1
  destination uri-to test2
!
dial-peer voice 32991 voip
  destination provision-policy 2000
  incoming called-number 1234
!

Device# show dialplan dialpeer 32991 number 2234 timeout

Macro Exp.: 2234
Enter Diversion header:sip:1234@cisco.com
Enter To header:sip:2234@10.0.0.0
VoiceOverIpPeer32134
  peer type = voice, system default peer = FALSE, information type = voice,
  description = `',

```

Step 3 show voice class dial-peer provision-policy

Displays a list of configured provision policies and associated rules.

Example:

```

Device# show voice class dial-peer provision-policy

Voice class dial-peer provision-policy: 100 AdminStatus: Up
Description: match only called

Pref  Policy Rule
----  -
1     called

Voice class dial-peer provision-policy: 101 AdminStatus: Up
Description: match both calling and called

Pref  Policy Rule
----  -
1     called calling

Voice class dial-peer provision-policy: 102 AdminStatus: Up
Description: match calling first; if no match then match called

Pref  Policy Rule
----  -
1     calling
2     called

Voice class dial-peer provision-policy: 200 AdminStatus: Up
Description: match referred-by and via uri; if no match then match request- uri

Pref  Policy Rule
----  -
1     referred-by via
2     uri

```

```

voice class dial-peer provision-policy: 300 AdminStatus: Up
  Description: match only request-uri

  Pref Policy Rule
  ----
  1 uri

Voice class dial-peer provision-policy: 400 AdminStatus: Up
  Description: match only request uri; if no match then match called

  Pref Policy Rule
  ----
  1 uri
  2 called

```

Configuration Example: Inbound Leg Headers for Outbound Dial-Peer Matching

Example: Configuring Inbound Called or Calling Numbers Used for Outbound Dial-Peer Matching

```

Device> enable
Device# configure terminal

Device(config)# voice class dial-peer provision-policy 200
Device(voice-class)# description match both calling and called
Device(voice-class)# preference 2 calling called
Device(voice-class)# exit

Device(config)# voice class e164-pattern-map 300
Device(voice-class)# description patterns
Device(voice-class)# e164 5557123
Device(voice-class)# e164 5558123
Device(voice-class)# e164 5559123
Device(voice-class)# exit

!Associating the Provision Policy with an Inbound Dial Peer
Device(config)# dial-peer voice 100 voip
Device(config-dial-peer)# destination provision-policy 200
Device(config-dial-peer)# end

!Associates a Pattern Map with an Outbound Dial Peer.
! The called number in the SIP headers of the inbound leg is matched to select the below
outbound dial peer.
Device(config)# dial-peer voice 200 voip
Device(config-dial-peer)# destination e164-pattern-map 300
Device(config-dial-peer)# end

```

Example: Configuring Inbound SIP Headers for Outbound Dial-Peer Matching

```

Device> enable
Device# configure terminal

```

```
Device(config)# voice class dial-peer provision-policy 200
Device(voice-class)# description match both calling and called
Device(voice-class)# preference 2 via from
Device(voice-class)# exit
```

!Associating the Provision Policy with an Inbound Dial Peer

```
Device(config)# dial-peer voice 100 voip
Device(config-dial-peer)# destination provision-policy 200
Device(config-dial-peer)# end
```

```
Device(config)# voice class uri 200 sip
Device(config-voice-uri-clas)# pattern 25054..
```

!Associates a Provision Policy with an Outbound Dial Peer.

The FROM SIP headers of the inbound leg is matched to select the below outbound dial peer.

```
Device(config)# dial-peer voice 200 voip
Device(config-dial-peer)# destination uri-from 200
Device(config-dial-peer)# end
```




CHAPTER 22

Server Groups

- [Overview, on page 207](#)
- [Configure Server Groups in Outbound Dial Peers, on page 209](#)
- [Configuration Examples for Server Groups in Outbound Dial Peers, on page 213](#)

Overview

This feature configures a server group (group of server addresses) that can be referenced from an outbound dial peer.

Server groups allow you to create simpler configurations by specifying a list of destination SIP servers for a single dial peer. When a call matches a dial peer that is configured with a server group, the destination is selected from the list of candidates based on a configured preference in the server group. If it is not possible to complete that call, the next candidate is selected. Alternatively, you can also choose to stop hunting through the group if a specified response code is received. If the call cannot be placed to any of the servers in the group, or hunting is stopped, call processing continues to the next preferred dial-peer.

You can configure server groups for SIP dial peers to include up to five IPv4 or IPv6 target server addresses listed in strict order of preference, or with equal weight for round robin or random selection. If a server-group is in the shutdown mode, all dial-peers using this destination are out of service.



Note Whenever destination server group is used, and multiple interfaces are involved, ensure that all servers in a group are reachable through the network to which the associated dial-peer is bound.

If there are session targets of different network, then different dial-peers must be created with appropriate grouping of the targets with respective binding of the interfaces.



- Note**
- You can use Server Groups only with SIP dial peers.
 - If a destination IP on the server group responds with codes 404, 500, or 503, the server group hunts for the next destination. But if the server group receives codes 480, 486, or 600, hunting is not supported and hence the server group does not hunt to the next destination. Further, the call fails.
-



Caution Huntstop is not allowed for the following set of cause codes 401, 407, 415, 417, 422, 480, 485, 486, and 488.

1. If you attempt to configure one of the listed cause codes specifically, the following CLI error message appears.

Example, huntstop 1 resp-code 401

Error: The specified response code cannot be used with Huntstop.

2. If you attempt to configure a range of codes that includes one of those listed, the command will be accepted with the following warning message.

Example, huntstop 1 resp-code 420 to 430

Warning: Range includes code(s) that will not stop hunting.



Note Load Balancing for DNS SRV Hosts can be used as an alternative to Server Groups.

Feature Information for Configuring Server Groups in Outbound Dial Peers

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 38: Feature Information for Configuring Server Groups in Outbound Dial Peers

Feature Name	Releases	Feature Information
Server Groups in Outbound Dial Peers	Cisco IOS XE Release 3.11S 15.4(1)T	This feature configures server groups (groups of IPv4 and IPv6 addresses) which can be referenced from an outbound SIP dial peer. The following command is introduced under: voice class server-group, description, ipv4 port preference, ipv6 port preference, hunt-scheme, show voice class server-group, shutdown (Server Group).

Feature Name	Releases	Feature Information
Hunt Stop for Server Groups	Cisco IOS XE Bengaluru 17.4.1a	<p>This feature allows you to configure hunt-stop based on (configurable) response codes in the Server Group.</p> <p>The following command is introduced under voice class server-group. huntstop rule-tag resp-code from_resp_code to to_resp_code</p>

Configure Server Groups in Outbound Dial Peers

Configure Server Groups in Outbound Dial Peers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class server-group** *server-group-id*
4. **{ipv4 | ipv6}** *address* [**port** *port*] [**preference** *preference-order*]
5. (Optional) **hunt-scheme round-robin**
6. (Optional) **description** *string*
7. (Optional) **huntstop rule-tag resp-code** *from_resp_code* **to** *to_resp_code*
8. **dial-peer voice** *dial-peer-id* **voip**
9. **session protocol sipv2**
10. **destination-pattern** [**+**] *string* [**T**]
11. **session server-group** *server-group-id*
12. **end**
13. **show voice class server-group** *server-group-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>voice class server-group <i>server-group-id</i></p> <p>Example:</p> <pre>Device(config)# voice class server-group 171</pre>	<p>Configures a voice class server group and enters voice class configuration mode.</p> <ul style="list-style-type: none"> You can use the shutdown command to make the server group inactive.
Step 4	<p>{ipv4 ipv6} <i>address</i> [port <i>port</i>] [preference <i>preference-order</i>]</p> <p>Example:</p> <pre>Device(config-class)# ipv4 10.1.1.1 preference 3</pre>	<p>Configures a server IP address as a part of this server group along with an optional port number and preference order.</p> <ul style="list-style-type: none"> Repeat this step to add up to five servers to the server group. The servers are not selected by the preference value if round robin is configured in the next step. Default and highest value of preference is zero.
Step 5	<p>(Optional) hunt-scheme round-robin</p> <p>Example:</p> <pre>Device(config-class)# hunt-scheme round-robin</pre>	<p>Defines a hunt method for the order of selection of target server IP addresses (from the IP addresses configured for this server group) for the setting up of outgoing calls.</p> <ul style="list-style-type: none"> If a hunt scheme is not defined, an available IP address of highest preference value is selected. If neither a round-robin hunt scheme nor a preference value is configured, the selection of servers is random.
Step 6	<p>(Optional) description <i>string</i></p> <p>Example:</p> <pre>Device(config-class)# description It has 3 entries</pre>	<p>Provides a description for the server group.</p>
Step 7	<p>(Optional) huntstop <i>rule-tag</i> resp-code <i>from_resp_code</i> <i>to_resp_code</i></p> <p>Example:</p> <p>You can configure hunting in 2 ways, providing the following cause codes -</p> <p>a. Range</p> <pre>Device(config-class)# huntstop 1 resp-code 400 to 410</pre> <p>b. Standalone</p> <pre>Device(config-class)# huntstop 2 resp-code 414</pre>	<p>Stops hunting for servers in the Server Group based on configurable response codes.</p> <ul style="list-style-type: none"> Huntstop rule identifier tags range: 1-1000. Configurable SIP error response codes range: 400 to 599. The range must be in between 400 and 599 and must be entered in minimum to maximum order (Example: 450 to 460). You can enter multiple ranges using additional instances of this command. Response codes do not need to be ordered between instances (Example: huntstop 1 500 to 510 and huntstop 2 400 to 450). <p>The following error message appears if there is an invalid input for SIP Response codes.</p> <pre>Error: Invalid SIP response code range configured for hunt-stop.</pre>

	Command or Action	Purpose
		<ul style="list-style-type: none"> Overlapping of SIP error response codes configuration is not permitted. For example, huntstop 1 resp-code 400 to 510. <p>The following error message appears if you try to configure the overlapping SIP error response codes.</p> <pre>Error: Overlap of response codes.</pre> <p>When one of the cause codes is in the configured range, the following warning message appears.</p> <p>Example, huntstop 1 resp-code 400 to 405</p> <pre>Warning: Range includes codes that will not stop hunting.</pre>
Step 8	dial-peer voice <i>dial-peer-id</i> voip Example: <pre>Device(config)# dial-peer voice 123 voip</pre>	Defines a VoIP dial peer and enters dial peer configuration mode.
Step 9	session protocol sipv2 Example: <pre>Device(config-dial-peer)# session protocol sipv2</pre>	Specifies SIP version 2 as the session protocol for calls between local and remote routers using the packet network.
Step 10	destination-pattern [+] <i>string</i> [T] Example: <pre>Device(config-dial-peer)# destination-pattern +5550179</pre>	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
Step 11	session server-group <i>server-group-id</i> Example: <pre>Device(config-dial-peer)# session server-group 171</pre>	<p>Configures the specified server group as the destination of the dial peer.</p> <ul style="list-style-type: none"> This command is available for SIP dial peers only. If the specified server group is in shutdown mode, the dial peer is not selected to route outgoing calls.
Step 12	end Example: <pre>Device(config-dial-peer)# end</pre>	Exits dial peer configuration mode and enters privileged EXEC mode.
Step 13	show voice class server-group <i>server-group-id</i> Example: <pre>Device# show voice class server-group 171</pre>	Displays information about the voice class server group.

Verify Server Groups in Outbound Dial Peers

SUMMARY STEPS

1. `show voice class server-group [server-group-id]`
2. `show running-config |section server-group`

DETAILED STEPS

Step 1 `show voice class server-group [server-group-id]`

The following example displays the configurations for all configured server groups or a specified server group.

Example:

```
Device# show voice class server-group 1

Voice class server-group: 1
  AdminStatus: Up           OperStatus: Up
  Hunt-Scheme: preference   Last returned server:
  Description: It has 3 entries
  Total server entries: 3

  Pref   Type   IP Address           IP Port
  ----   -
  1      ipv4   10.1.1.1             -----
  2      ipv4   10.1.1.2
  3      ipv4   10.1.1.3

-----

Total Huntstop tags: 2
Tag ID From Response code   To Response code
-----
  1      404                       404
  2      410                       599
-----
```

The following example displays the configurations for dial peers that are associated with server groups.

Example:

```
Device# show voice class server-group dialpeer 1

Voice class server-group: 1   AdminStatus: Up
  Hunt-Scheme: preference
  Total Remote Targets: 3

  Pref   Type   IP Address           IP Port
  ----   -
  1      ipv4   10.1.1.1             -----
  2      ipv4   10.1.1.2
  3      ipv4   10.1.1.3
```

Step 2 `show running-config |section server-group`

The following example displays the running configuration for server groups.

Example:

```
Device#show running-config | section server-group
voice class server-group 1
```

```

ipv4 10.1.1.1 preference 1
ipv4 10.1.1.2 preference 2
ipv4 10.1.1.3 preference 3
description It has 3 entries
huntstop 1 resp-code 404 to 404
huntstop 2 resp-code 410 to 599
voice class server-group 2
ipv4 10.1.1.1
ipv4 10.1.1.2
ipv4 10.1.1.3
description It has 3 entries
hunt-scheme round-robin
huntstop 1 resp-code 401 to 599

```

Configuration Examples for Server Groups in Outbound Dial Peers

Server Groups in Outbound Dial Peers (Preference-Based Selection)

```

! Configuring the Server Group
Device(config)# voice class server-group 1
Device(config-class)# ipv4 10.1.1.1 preference 1
Device(config-class)# ipv4 10.1.1.2 preference 2
Device(config-class)# ipv4 10.1.1.3 preference 3
Device(config-class)# description It has 3 entries
Device (config-class)# huntstop 1 resp-code 404
Device(config-class)# huntstop 2 resp-code 410 to 599
Device(config-class)# exit

! Configuring an outbound SIP dial peer.
Device(config)# dial-peer voice 1 voip
!Associate a destination pattern
Device(config-dial-peer)# destination-pattern 3001
Device(config-dial-peer)# session protocol sipv2
!Associate a server group with the dial peer
Device(config-dial-peer)# session server-group 1
Device(config-dial-peer)# end

! Displays the configurations made for the outbound dial peer 181 associated with a server
group
Device# show voice class server-group dialpeer 1

Voice class server-group: 1      AdminStatus: Up
  Hunt-Scheme: preference
  Total Remote Targets: 3

  Pref   Type   IP Address           IP Port
  ----   -
  1      ipv4   10.1.1.1
  2      ipv4   10.1.1.2
  3      ipv4   10.1.1.3

! Displays the configurations made for the server group.

```

```

Device# show voice class server-group 1

Voice class server-group: 1
  AdminStatus: Up                OperStatus: Up
  Hunt-Scheme: preference        Last returned server:
  Description: It has 3 entries
  Total server entries: 3

  Pref   Type   IP Address          IP Port
  ----   -
  1      ipv4   10.1.1.1           -----
  2      ipv4   10.1.1.2
  3      ipv4   10.1.1.3

-----

Total Huntstop tags: 2
Tag ID From Response code      To Response code
-----
  1      404
  2      410
-----

```

Server Groups in Outbound Dial Peers (Round-Robin-Based Selection)

```

! Configuring the Server Group
Device(config)# voice class server-group 2
Device(config-class)# ipv4 10.1.1.1
Device(config-class)# ipv4 10.1.1.2
Device(config-class)# ipv4 10.1.1.3
Device(config-class)# hunt-scheme round-robin
Device(config-class)# huntstop 1 resp-code 401 to 599
Device(config-class)# description It has 3 entries
Device(config-class)# exit

! Configuring an outbound SIP dial peer.
Device(config)# dial-peer voice 2 voip
! Associate a destination pattern
Device(config-dial-peer)# destination-pattern 3001
Device(config-dial-peer)# session protocol sipv2
! Associate a server group with the dial peer
Device(config-dial-peer)# session server-group 2
Device(config-dial-peer)# end

! Displays the configurations made for the outbound dial peer 181 associated with a server
group
Device# show voice class server-group dialpeer 2

Voice class server-group: 2      AdminStatus: Up
  Hunt-Scheme: round-robin
  Total Remote Targets: 3

  Pref   Type   IP Address          IP Port
  ----   -
  0      ipv4   10.1.1.3           -----
  0      ipv4   10.1.1.1
  0      ipv4   10.1.1.2

! Displays the configurations made for the server group.
Device# show voice class server-group 2

```



```
Voice class server-group: 2
AdminStatus: Up           OperStatus: Up
Hunt-Scheme: round-robin  Last returned server: 10.1.1.2
Description: It has 3 entries
Total server entries: 3
```

Pref	Type	IP Address	IP Port
0	ipv4	10.1.1.1	
0	ipv4	10.1.1.2	
0	ipv4	10.1.1.3	

```
-----
Total Huntstop tags: 1
Tag ID From Response code      To Response code
-----
1      401                      599
-----
```




CHAPTER 23

Domain-Based Routing

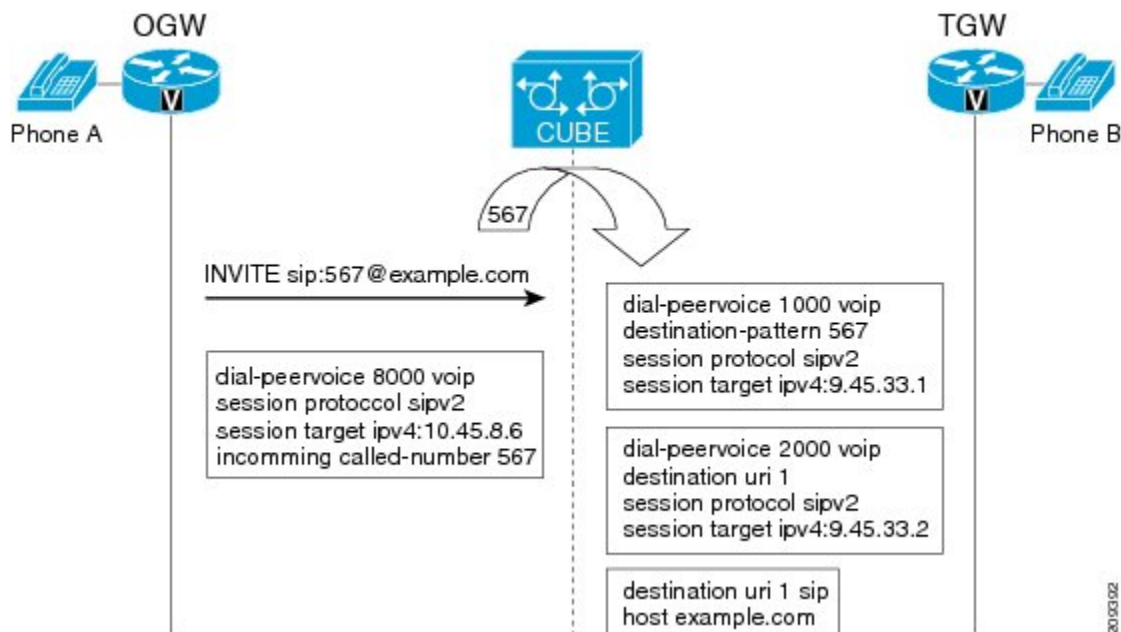
- [Overview, on page 217](#)
- [Configure Domain-Based Routing, on page 219](#)
- [Configuration Examples for Domain-Based Routing, on page 223](#)

Overview

The Domain-based routing feature provides support for matching an outbound dial peer based on the domain name or IP address provided in the request URI of the incoming SIP message or an inbound dial peer.

Domain-based routing enables for calls to be routed on the outbound dialpeer based on the domain name or IP address provided in the request Uniform Resource Identifier (URI) of incoming Session IP message.

When a dial peer has an application configured as a session application, then only the user parameter of the request URI is used and is sent from the inbound SIP SPI to the application. The session application performs a match on an outbound dial peer based on the user parameter of the request URI sent from the inbound dial peer. In the figure below, 567 is the user portion of the request-URI that is passed from the inbound dial peer to the application and the matching outbound dial-peer found is 1000.



With the introduction of the domain-based routing feature, all parameters including the domain name of the request URI will be sent to the application and the outbound dial peer can be matched with any parameter. In Figure 1, when the domain name example.com is used to match an outbound dial peer the resulting dial peer is 2000. The **call route url** command is used for configuring domain-based routing.



Note Whenever using the **call route url** command, apply translation rule at outbound dial-peer not in to call-route url.

Domain-based routing support is available only for SIP-SIP call flows.

Feature Information

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 software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Table 39: Feature Information for Domain-Based Routing Support on the CUBE

Feature Name	Releases	Feature Information
Domain Based Routing Support on the CUBE	15.2(1)T Cisco IOS XE Release 3.8S	The domain-based routing enables for calls to be routed on the outbound dial peer based on the domain name or IP address provided in the request URI (Uniform Resource Identifier) of incoming SIP message. The following commands were introduced or modified: call-route , voice-class sip call-route .

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. © 2011 Cisco Systems, Inc. All rights reserved

Configure Domain-Based Routing

Configure Domain-Based Routing at Global Level

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. call-route url
6. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice service configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# sip	Enters voice service SIP configuration mode.
Step 5	call-route url Example: Device(conf-serv-sip)# call-route url Example:	Routes calls based on the URL.
Step 6	exit Example: Device(conf-serv-sip)# exit	Exits the current mode.

Configure Domain-Based Routing at Dial Peer Level

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice dial-peer tag voip`
4. `voice-class sip call-route url`
5. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice dial-peer tag voip Example: Device(config)# dial-peer voice 2 voip	Enter dial peer voice configuration mode.
Step 4	voice-class sip call-route url Example: Device(config-dial-peer)# Example: Routes calls based on the URL	
Step 5	exit Example: Device(config-dial-peer)# exit	Exits the current mode.

Verify and Troubleshoot Domain-Based Routing

Use this procedure to verify and troubleshoot domain-based routing on CUBE.

SUMMARY STEPS

1. `enable`
2. `debug ccsip all`
3. `debug voip dialpeer inout`


```
*May 1 19:32:11.731: //-1/6372E2598012/DPM/dpAssociateIncomingPeerCore:
  Calling Number=4085550111, Called Number=3600, Voice-Interface=0x0,
  Timeout=TRUE, Peer Encap Type=ENCAP_VOIP, Peer Search Type=PEER_TYPE_VOICE,
  Peer Info Type=DIALPEER_INFO_SPEECH
*May 1 19:32:11.731: //-1/6372E2598012/DPM/dpAssociateIncomingPeerCore:
  Result=Success(0) after DP_MATCH_INCOMING_DNIS; Incoming Dial-peer=100
*May 1 19:32:11.735: //-1/6372E2598012/DPM/dpMatchPeersCore:
  Calling Number=, Called Number=3600, Peer Info Type=DIALPEER_INFO_SPEECH
*May 1 19:32:11.735: //-1/6372E2598012/DPM/dpMatchPeersCore:
  Match Rule=DP_MATCH_DEST; Called Number=3600
*May 1 19:32:11.735: //-1/6372E2598012/DPM/dpMatchPeersCore:
  Result=Success(0) after DP_MATCH_DEST
*May 1 19:32:11.735: //-1/6372E2598012/DPM/dpMatchPeersMoreArg:
  Result=SUCCESS(0)
```

The following event shows the matched dial peers in the order of priority:

Example:

```
List of Matched Outgoing Dial-peer(s):
  1: Dial-peer Tag=3600
  2: Dial-peer Tag=36
```

Configuration Examples for Domain-Based Routing

Example Configuring Domain-Based Routing

The following example shows how to enable domain-based routing support on the CUBE:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# call-route url
Device(conf-serv-sip)# exit
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# voice-class sip call-route url
Device(config-dial-peer)# exit
```




CHAPTER 24

ENUM Enhancement per Kaplan Draft RFC

- [Overview, on page 225](#)
- [Restrictions, on page 226](#)
- [Configure ENUM, on page 227](#)
- [Troubleshooting Tips, on page 229](#)
- [Configuration Examples for ENUM Enhancement per Kaplan Draft RFC, on page 230](#)

Overview

The Cisco Unified Border Element (CUBE) facilitates the mapping of E.164 called numbers to Session Initiation Protocol (SIP) Uniform Resource Identifiers (URIs). The SIP ENUM technology allows the traditional telephony part of the network (using E.164 numbering to address destinations) to interwork with the SIP telephony part of the network, generally using SIP URIs. From the Public Switched Telephone Network (PSTN) network, if an end user dials an E.164 called party, the number can be translated by an ENUM gateway into the corresponding SIP URI. This SIP URI is then used to look up the Domain Name System (DNS) Naming Authority Pointer (NAPTR) Resource Records (RR). The NAPTR RR (as defined in RFC 2915) describes how the call should be forwarded or terminated and records information, such as email addresses, a fax number, a personal website, a VoIP number, mobile phone numbers, voicemail systems, IP-telephony addresses, and web pages. Alternately, when the calling party is a VoIP endpoint and dials an E.164 number, then the originator's SIP user agent (UA) converts it into a SIP URI to be used to look up at the ENUM gateway DNS and fetch the NAPTR RR.

The ENUM enhancement per Kaplan draft RFC provides source-based routing, that is, SIP-to-SIP calls can be routed based on the source SIP requests. To provide source-based routing and to interact with the Policy Server, an EDNS0 OPT pseudo resource record with source URI, incoming SIP call ID, outbound SIP call ID, and Call Session Identification are added to the ENUM DNS query, according to **draft-kaplan-enum-sip-routing-04**. The incoming SIP call ID, outbound SIP call ID, and Call Session Identification are automatically included with an EDNS0 OPT pseudo resource record in the ENUM DNS query only if “source-uri no-cache” is enabled and XCC service is registered. This feature also provides the flexibility to disable route caching.

SIP-to-SIP calls can be routed based on the source SIP requests, using the ENUM enhancement feature. To provide source-based routing and to interact with Policy Server, an EDNS0 OPT pseudo resource record with source URI, incoming SIP call ID, outbound SIP call ID, and Call session Identification are added to the ENUM DNS query. The DNS server filters its response based on the source URI and call ID information and returns the appropriate NAPTR entries. To enable this feature, you must use the **source-uri** option in the **voice enum-match-table <table-number>** command. In addition, you can use the **no-cache** option to disable caching.

Refer to RFC 3761 and **draft-kaplan-enum-sip-routing-04** for more information about routing SIP requests with ENUM.

Feature Information for ENUM Enhancement per Kaplan Draft RFC

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 40: Feature Information for ENUM Enhancement per Kaplan Draft RFC

Feature Name	Releases	Feature Information
ENUM Enhancement per Kaplan Draft RFC	Cisco IOS XE 3.14S Cisco IOS 15.5(1)T	The ENUM enhancement per Kaplan draft RFC provides source-based routing, that is, SIP-to-SIP calls can be routed based on the source SIP requests. To provide this source-based routing, an EDNS0 OPT pseudo resource record with source URI is added to the ENUM DNS query, according to draft-kaplan-enum-sip-routing-04 . This feature also provides the flexibility to disable route caching.
Support to include inbound call ID, outbound call ID and Call Session Identification to ENUM DNS query	Cisco IOS 15.5(2)T Cisco IOS XE 3.15S	This feature allows you to add incoming SIP call ID, outbound SIP call ID, and Call Session Identification to an EDNS0 OPT pseudo resource record in the ENUM DNS query.

Restrictions

- Supported only for SIP-to-SIP calls.
- The full command of **voice enum-match-table**, including the options, needs to be specified whenever being referenced by its subcommand. If not, the defaults, **no source-uri** and **no no-cached** (or **caching**) will take effect.
- As the maximum number of characters of the host shown in the **show host** command is 25, the source URI may not be displayed completely.
- The source URI is displayed in a separate line below, starting with “source-uri=”. Refer to the **show** command outputs in this chapter.
- If **no-cache** is configured in the **voice enum-match-table**, no cache table look-up would be made and hence an ENUM query would be made regardless of what is in the cache table.
- Both the target and source, where the source can be null/undefined or defined, need to be matched when looking up the cache table.
- The OPT RR will be added to the query for a SIP-to-SIP call only if the **source-uri** is configured for the outbound **enum-match-table**.

- The route will not be cached if the server does not support the OPT RR (it is recommended to remove the **source-uri** for this scenario if caching is preferred).
- The source URL can be prefixed with a host/target in the host name field in a double quote in the **show host host** command to display routes for the host specific with this source.
- A wild card, “*”, can be used to denote “all” hosts in the **show host** command. It can be by itself or any host matched with its prefix. The prefix can be a host name, partial or complete, or a domain name with partial or complete source URL.

Refer to the document titled [Cisco Unified Border Element ENUM Support Configuration Example](#) for a detailed message format.

Configure ENUM

Enable Source-Based Routing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice enum-match-table** *match-table-index* [**source-uri**] [**no-cache**]
4. **end**

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	voice enum-match-table <i>match-table-index</i> [source-uri] [no-cache] Example: Device(config)# voice enum-match-table 5 source-uri no-cache	Enables source URI filtering for the enum match table entry. You can use the no-cache option to disable the caching to the voice enum command.
Step 4	end Example: Device(config-enum)# end	Returns to privileged EXEC mode.

Test the ENUM Request

To test the ENUM request, you can use the **source-uri** option so that the source-based routing enum can be tested.

SUMMARY STEPS

1. **enable**
2. **test enum match-table-index input -pattern source-uri source-uri more parameter**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	test enum match-table-index input -pattern source-uri source-uri more parameter Example: Device# test enum 1117777 source sip:1116666@10.1.50.16 more "ibcall-id=1-23735@10.1.50.16; obcall-id=7190DF-F1AA3CF1@10.1.110.222;sbc-id=1	Tests the source-based routing ENUM. <ul style="list-style-type: none"> • The source routing or no caching features depend on the voice enum-match-table command. If the source-uri command is not configured, the source-uri source-uri in the test command is ignored.
Step 3	end Example: Device# end	Returns to privileged EXEC mode.

Verify the ENUM Request

Use the following show commands to verify your network setup. You can compare the output of these commands to the output of the ENUM test in order to verify that ENUM is working.

SUMMARY STEPS

1. **show host ***
2. **show host 1.0.9.3.e164-test***
3. **show host 1***
4. **show host "1.0.9.3.e164-test sip*"**

DETAILED STEPS

Step 1 **show host ***
Example:

```
Device# show host *
```

```
Host          Port      Flags      Age Type  Address(es)
ns.e164-test  None      (temp, OK) 0   IP    127.0.0.1
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:5403@1.4.65.5"
1.1.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:5403@1.4.65.5"
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:3401@1.4.65.5"
```

Step 2 show host 1.0.9.3.e164-test*

Example:

```
Device# show host 1.0.9.3.e164-test*
```

```
Host          Port      Flags      Age Type  Address(es)
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:5403@1.4.65.5"
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:3401@1.4.65.5"
```

Step 3 show host 1*

Example:

```
Device# show host 1*
```

```
Host          Port      Flags      Age Type  Address(es)
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:5403@1.4.65.5"
1.1.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:5403@1.4.65.5"
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:3401@1.4.65.5"
```

Step 4 show host "1.0.9.3.e164-test sip*"

Example:

```
Device# show host "1.0.9.3.e164-test sip*"
```

```
Host          Port      Flags      Age Type  Address(es)
ns.e164-test  None      (temp, OK) 0   IP    127.0.0.1
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:5403@1.4.65.5"
1.0.9.3.e164-test sip:540 NA (temp, OK) 0   NAPTR 0 0 U sip+E2U /^.*$/sip:3901@10.1.18.28/
Source-uri="sip:3401@1.4.65.5"
```

Troubleshooting Tips

Use the following commands for debugging information:

- **debug voip enum detail**

- **debug ip domain**
- **debug ccsip message**
- **debug voip ccapi inout**
- **clear voip fpi session correlator-id**—This command is used to clear the hung FPI sessions. After the hung session is identified using the existing **show** commands and its correlator is obtained, the **clear voip fpi session correlator-id** command can be used to clear the session.

Use the following **show** command that is helpful for debugging:

- **show host** [**all** | * | *host-name* | *partial -host -name**]

Below is an extract of a sample ENUM DNS query containing the EDNS0 OPT pseudo resource record fields as per Kaplan Draft that is helpful in debugging. In the below query the values corresponding to ibcall-id, obcall-id, and sbc-id represent the incoming SIP call ID, outbound SIP call ID and Call Session Identification respectively.

```
7.7.7.7.1.1.1.e164.arpa sip:1116666@10.1.50.16enum_dns_query: name = 7.7.7.7.1.1.1.e164.arpa
sip:1116666@10.1.50.16 type = 35, ns_server = 0x0 no_cache 1 more_data
;ibcall-id=1-23735@10.1.50.16;
obcall-id=7190DF-39DD11E4-8008EDAD-F1AA3CF1@10.1.110.222;sbc-id=1
```

Configuration Examples for ENUM Enhancement per Kaplan Draft RFC

```
voice enum-match-table 1 source-uri //The source URI is sent to the DNS server to filter
the route.//
  description enable source-uri
  rule 2 1 /^\(.*\)$/ /\1/ e164.arpa

voice enum-match-table 2 source-uri no-cache
rule 1 1 /^\(.*\)$/ /\1/ e164-test

voice enum-match-table 3 no-cache //The cache table is not looked up and the route is not
cached.//
  rule 1 1 /^\(.*\)$/ /\1/ e164-test
```

The following is a sample configuration for the ENUM enhancement feature:

```
dial-peer voice 1 voip
  description ENUM Inbound dialpeer
  session protocol sipv2
  incoming called-number 1116666

dial-peer voice 2 voip
  description ENUM Outbound dialpeer
  destination-pattern 1117777
  session protocol sipv2
  session target enum:1 //Session target configured to look up ENUM table 1.//
```




PART **V**

SIP Header Manipulation

- [Manipulate SIP Status-Line Header of SIP Responses, on page 233](#)
- [Copy SIP Headers, on page 239](#)
- [SIP Profiles, on page 245](#)
- [Pass Unsupported SIP Headers, on page 273](#)



CHAPTER 25

Manipulate SIP Status-Line Header of SIP Responses

- [Manipulat SIP Status-Line Header of SIP Responses, on page 233](#)
- [Copy Incoming SIP Response Status Line to Outgoing SIP Response, on page 234](#)
- [Modify Status-Line Header of Outgoing SIP Response with User Defined Values, on page 237](#)

Manipulat SIP Status-Line Header of SIP Responses

The SIP status line is a SIP response header, and it can be modified like any other SIP headers of a message. it can either be modified with a user-defined value, or the status line from an incoming response can be copied to an outgoing SIP response. The SIP header keyword used for the response status line is **SIP-StatusLine**.

Feature Information

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.

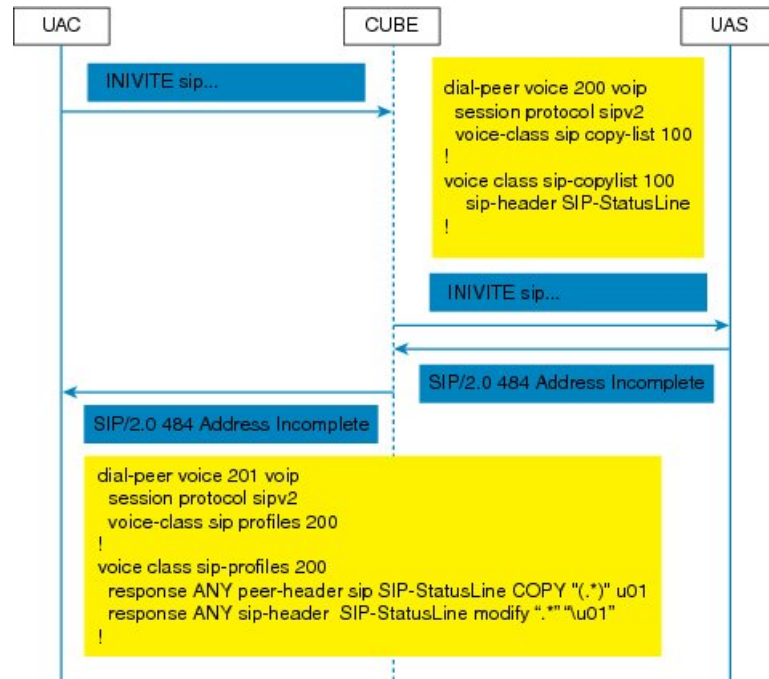
Table 41: Feature Information for Manipulating SIP Responses

Feature Name	Releases	Feature Information
SIP Profile Enhancements for SIP responses and error codes	Baseline Functionality	<p>This feature extends SIP profiles to allow the following:</p> <ul style="list-style-type: none"> • Modification of the outgoing SIP response status line. Previously, only modification of outgoing SIP requests and responses was possible. • Copying of the incoming SIP response status-line. The information from the peer-leg status-line can then be copied to user-variables and applied to the outbound response status-line. This option can be used to pass-thru the error-code and error phrase from peer-leg. Previously, only copying of SIP headers were possible. • Before applying a SIP profile to a response from CUBE, the response can be mapped to its corresponding request.

Copy Incoming SIP Response Status Line to Outgoing SIP Response

To copy content from the status line of an incoming SIP response that a device receives to an outgoing response, configure a SIP copylist for SIP status line and apply it to an incoming dial peer. A SIP profile must be configured to copy the status line of an incoming SIP response to a user-defined variable and apply it to an outgoing SIP response.

Figure 18: Call Flow for Copying the Status Line from the Incoming SIP Response to the Outgoing SIP Response



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-copylist tag**
4. **sip-header SIP-StatusLine**
5. **exit**
6. **dial-peer voice inbound-dial-peer-id voip**
7. **voice-class sip copy-list list-id**
8. **exit**
9. **voice class sip-profiles tag**
10. **response response-code peer-header sip SIP-StatusLine copy match-pattern copy-variable**
11. **response response-code sip-header SIP-StatusLine modify match-pattern copy-variable**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

Copy Incoming SIP Response Status Line to Outgoing SIP Response

	Command or Action	Purpose
	Device# configure terminal	
Step 3	voice class sip-copylist tag Example: Device(config)# voice class sip-copylist 1	Configures a list of entities to be sent to the peer call leg and enters voice class configuration mode.
Step 4	sip-header SIP-StatusLine Example: Device(config-class)# sip-header SIP-StatusLine	Specifies that the Session Initiation Protocol (SIP) status line header must be sent to the peer call leg.
Step 5	exit Example: Device(config-class)# exit	Exits voice class configuration mode and returns to global configuration mode.
Step 6	dial-peer voice inbound-dial-peer-id voip Example: Device(config)# dial-peer voice 99 voip	Specifies an inbound dial peer and enters dial peer configuration mode.
Step 7	voice-class sip copy-list list-id Example: Device(config-dial-peer)# voice-class sip copy-list 1	Associates the SIP copy list with the inbound dial peer.
Step 8	exit Example: Device(config-dial-peer)# exit	Exits dial peer configuration mode and returns to global configuration mode.
Step 9	voice class sip-profiles tag Example: Device(config)# voice class sip-profiles 10	Enables dial peer-based VoIP SIP profile configurations and enters voice class configuration mode.
Step 10	response response-code peer-header sip SIP-StatusLine copy match-pattern copy-variable Example: Device(config-class)# response ANY peer-header sip SIP-StatusLine copy "(.*)" u01	Copies responses from the corresponding incoming call leg into a copy variable.
Step 11	response response-code sip-header SIP-StatusLine modify match-pattern copy-variable Example: Device(config-class)# response ANY sip-header SIP-StatusLine modify ".*" "\u01"	Modifies an outgoing response using the copy variable defined in the previous step.

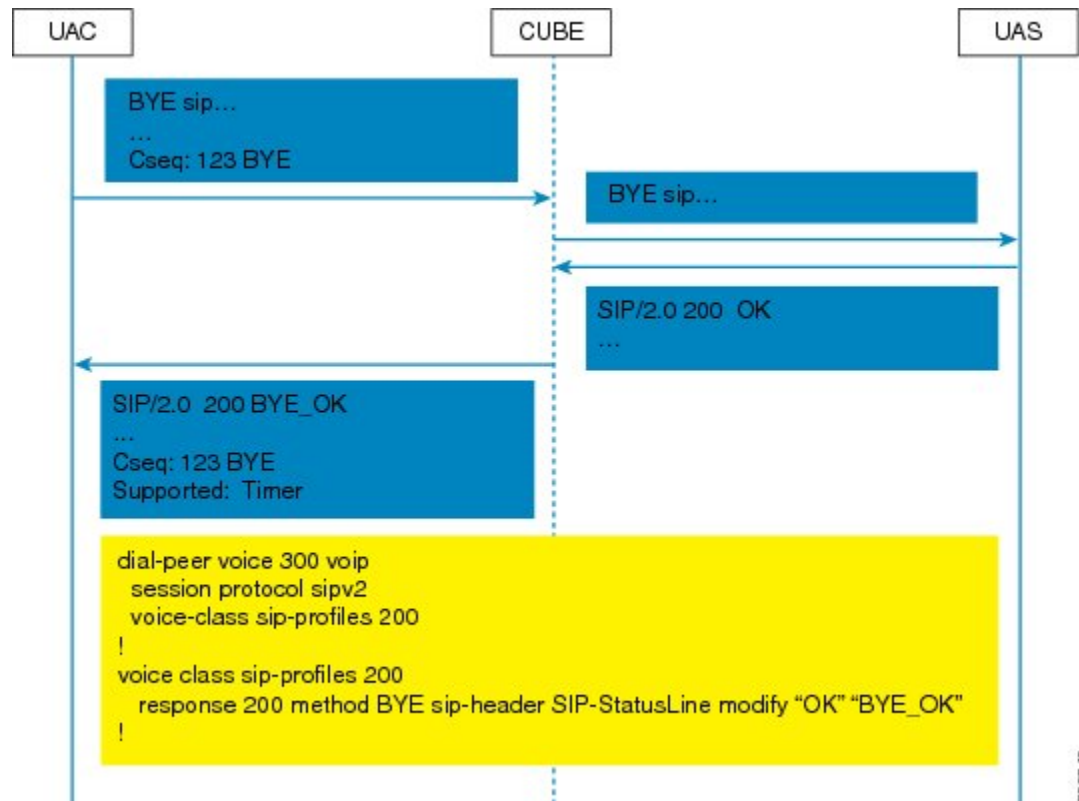
	Command or Action	Purpose
Step 12	exit Example: Device(config-class)# exit	Exits voice class configuration mode and returns to global configuration mode.

What to do next

Apply the SIP profile to the outbound dial peer to copy the SIP response to the outbound leg.

Modify Status-Line Header of Outgoing SIP Response with User Defined Values

Figure 19: Call Flow Configuring a New Status Line for an Outgoing SIP Response Based on an Incoming SIP Request



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-profiles tag**

4. **response** *response-code* [**method** *method-type*] **sip-header** **SIP-StatusLine** **modify** *match-pattern* *replacement-pattern*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class sip-profiles <i>tag</i> Example: Device(config)# voice class sip-profiles 10	Enables dial peer-based VoIP SIP profile configurations and enters voice class configuration mode.
Step 4	response <i>response-code</i> [method <i>method-type</i>] sip-header SIP-StatusLine modify <i>match-pattern</i> <i>replacement-pattern</i> Example: Modifying status line of a SIP header to a user-defined response type: Device(config-class)# response 404 sip-header SIP-StatusLine modify "404 Not Found" "404 MyError"	Modifies SIP status line of a SIP response with user-defined values.
Step 5	exit Example: Device(config-class)# exit	Exits voice class configuration mode.

What to do next

Associate the SIP profile with an outbound dial peer.



CHAPTER 26

Copy SIP Headers

- Copy SIP Headers, on page 239
- Copy SIP Header Fields to Another, on page 239
- Example: Copying the To Header into the SIP-Req-URI, on page 243

Copy SIP Headers

This feature shows you how outgoing SIP headers can be manipulated using information from incoming and other outgoing SIP headers.

Feature Information

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 42: Feature Information for Copying with SIP Profiles

Feature Name	Releases	Feature Information
Support for conditional header manipulation of SIP headers	Baseline Functionality	This feature modifies the following commands: voice class sip-profiles, response, request, voice-class sip copy-list, sip-header

Copy SIP Header Fields to Another

Copy From an Incoming Header and Modifying an Outgoing Header

To copy content from an incoming header that a device receives to an outgoing header, configure a SIP copylist for that header and apply it to an incoming dial peer. A SIP profile is configured to copy this incoming header to a user-defined variable and apply it to an outgoing header.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-copylist tag**
4. Do one of the following:
 - **sip-header header-name**
 - **sip-header SIP-Req-URI**
5. **exit**
6. **dial-peer voice inbound-dial-peer-tag voip**
7. **voice-class sip-copylist tag**
8. **exit**
9. **voice class sip-profiles profile-id**
10. **{request | response} message peer-header sip header-to-copy copy header-value-to-match copy-variable**
11. **{request | response} message {sip-header | sdp-header} header-to-modify modify header-value-to-match header-value-to-replace**
12. **exit**
13. **dial-peer voice outbound-dial-peer-tag voip**
14. **voice-class sip-profiles profile-id**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	voice class sip-copylist tag Example: Device(config)# voice class sip-copylist 100	Configures a list of entities to be sent to a peer call leg and enters voice class configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> • sip-header header-name • sip-header SIP-Req-URI Example: Device(config-class)# sip-header To	Specifies the SIP header to be copied to the peer call leg. <ul style="list-style-type: none"> • sip-req-uri—Configures Cisco Unified Border Element (UBE) to send a SIP request Uniform Resource Identifier (URI) to the peer call leg. • header-name—Configures Cisco Unified Border Element (UBE) to send the header name specified to the peer call leg.
Step 5	exit	Exits voice class configuration mode.

	Command or Action	Purpose
Step 6	dial-peer voice <i>inbound-dial-peer-tag</i> voip Example: Device(config)# dial-peer voice 2 voip	Enters the dial peer configuration mode for the specified inbound dial peer.
Step 7	voice-class sip-copylist <i>tag</i> Example: Device(config-dial-peer)# voice-class sip-copylist 100	Applies the copy list to the dial-peer.
Step 8	exit	Exits to global configuration mode.
Step 9	voice class sip-profiles <i>profile-id</i> Example: Device(config)# voice class sip-profiles 10	Create a SIP Profile and enters voice class configuration mode.
Step 10	{request response} message peer-header sip header-to-copy copy header-value-to-match copy-variable Example: Device(config-class)# request INVITE peer-header sip TO copy "sip:(.*)@" u01	Copies headers from the corresponding incoming dial peer into a copy variable.
Step 11	{request response} message {sip-header sdp-header} header-to-modify modify header-value-to-match header-value-to-replace Example: Device(config-class)# request INVITE sip-header SIP-Req-URI modify ".*@(.*)" "INVITE sip:\u01@\1"	Modifies an outgoing SIP or SDP header using the copy variable defined in the previous step.
Step 12	exit	Exits to global configuration mode.
Step 13	dial-peer voice <i>outbound-dial-peer-tag</i> voip Example: Device(config)# dial-peer voice 2 voip	Enters the dial peer configuration mode for the specified outbound dial peer.
Step 14	voice-class sip-profiles <i>profile-id</i> Example: Device(config-dial-peer)# voice-class sip-profiles 10	SIP Profile is applied to the dial-peer.
Step 15	exit	Exits to global configuration mode.

Copy From One Outgoing Header to Another

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-profiles** *profile-id*
4. **{request | response} message {sip-header | sdp-header} header-to-copy copy header-value-to-match copy-variable**
5. **{request | response} message {sip-header | sdp-header} header-to-modify modify header-value-to-match header-value-to-replace**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	voice class sip-profiles <i>profile-id</i> Example: Device(config)# voice class sip-profiles 10	Creates a SIP profile and enters voice class configuration mode.
Step 4	{request response} message {sip-header sdp-header} header-to-copy copy header-value-to-match copy-variable Example: Device(config-class)# request INVITE sip-header TO copy "sip:(.*)@" u01	Copies the contents of the specified header from an outbound message into a copy variable.
Step 5	{request response} message {sip-header sdp-header} header-to-modify modify header-value-to-match header-value-to-replace Example: Device(config-class)# request INVITE sip-header SIP-Req-URI modify ".*@(.*)" "INVITE sip:\u01@1"	Modifies an outgoing SIP or SDP header using the copy variable defined in the previous step.
Step 6	end Example: Device(config-class)# end	Exits voice class configuration mode and enters privileged EXEC mode.

What to do next

Apply the SIP Profile to an outbound dial peer.

Example: Copying the To Header into the SIP-Req-URI

Copying Contents from One Header to Another

Given below is a scenario in an organization, where the provider has sent only a global reference number in the SIP-Req-URI header of the INVITE message, and has placed the actual phone destination number only in the To: SIP header. The CUCM typically routes on the SIP-Req-URI.



Given below is the original SIP message, where the INVITE has a non-routable value of 43565432A5. The actual phone destination number is 2555552 and is present in the To: SIP header.

Figure 20: Incoming SIP Message

```
INVITE sip:43565432A5@192.168.1.100:5060 SIP/2.0
From: <sip:027784200@A.eu;user=phone>;
To: <sip:2555552@A.eu>
...
```

Given below is the SIP message that is required. Note that 43565432A5 has changed to 2555552 in the SIP INVITE.

Figure 21: Modified SIP Message

```
INVITE sip:2555552@192.168.1.100:5060 SIP/2.0
From: <sip:027784200@A.eu;user=phone>;
To: <sip:2555552@A.eu>
...
```

Because CUBE is a back-to-back user agent, the incoming dial peer is matched to the outgoing dial peer. The SIP Profile configured below copies the value from the incoming dial peer

```
Device# voice class sip-profiles 1

!Copy the To header from the incoming dial peer into variable u01
Device(config-class)# request INVITE peer-header sip TO copy "sip:(.*)@" u01

!Modify the outgoing SIP Invite with this variable.
Device(config-class)# request INVITE sip-header SIP-Req-URI modify ".*(.*)" "INVITE
sip:\u01@\1"
```

Apply the SIP profile to the incoming dial peer.

```
Device(config)# dial-peer voice 99 voip
Device(config-dial-peer)# outgoing to CUCM
Device(config-dial-peer)# destination-pattern 02555555.
Device(config-dial-peer)# session protocol sip2
```

Example: Copying the To Header into the SIP-Req-URI

```
Device(config-dial-peer)# session target ipv4:10.1.2.3

!Applying SIP profile to the dial peer
Device(config-dial-peer)# voice-class sip profiles 1
Device(config-dial-peer)# voice-class code 1
Device(config-dial-peer)# dtmf-relay rtp-nte
Device(config-dial-peer)# no vad
```

Additionally, if you would like to copy the To: Header from the inbound dial peer to the outbound dial peer, use a copy list.

```
!Create a copy List
Device(config)# voice class sip-copylist 1
Device(config-class)# sip-header TO
Device(config-class)# exit

!Apply the copy list to incoming dial peer.
Device(config)# dial-peer voice 1 voip
Device(config-dial-peer)# description incoming SIP Trunk
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target sip-server
Device(config-dial-peer)# incoming uri to TRUNK
Device(config-dial-peer)# voice-class code 1
Device(config-dial-peer)# voice-class sip copy-list 1

Device(config)# voice class uri TRUNK sip
Device(config-class)# user-id 2555555.
Device(config-class)# end
```



CHAPTER 27

SIP Profiles

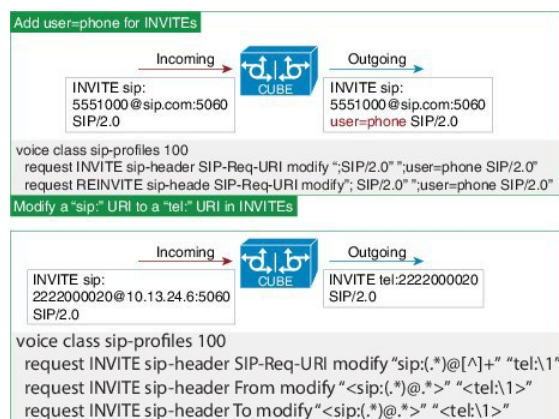
- [Overview, on page 245](#)
- [Restrictions, on page 248](#)
- [How to Configure SIP Profiles, on page 249](#)
- [Supported SIP Messages, on page 258](#)
- [Verify SIP Profiles, on page 262](#)
- [Troubleshoot SIP Profiles, on page 262](#)
- [Examples: Adding, Modifying, Removing SIP Profiles, on page 263](#)

Overview

Protocol translation and repair are a key Cisco Unified Border Element (CUBE) function. CUBE can be deployed between two incompatible SIP devices to normalize messaging, ensuring end-to-end compatibility.

Service providers may have policies for which SIP messaging fields should be present (and the values they contain) before a SIP call enters their network. Similarly, enterprises and small businesses may have policies for the information that can enter or exit their networks for policy or security reasons from a service provider SIP trunk.

Figure 22: SIP Profile



CUBE Session Initiation Protocol (SIP) profiles change SIP incoming or outgoing messages so that interoperability between incompatible devices can be ensured.

You can configure SIP profiles with rules to add, remove, copy, or modify the SIP, Session Description Protocol (SDP), and peer headers that enter or leave CUBE. The rules in a SIP profile configuration can also be tagged with a unique number. Tagging the rules allows you to insert or delete rules at any position of the existing SIP profile configuration without deleting and reconfiguring the entire voice-class sip profile.

Figure 23: Incoming and Outgoing Messages Where SIP Profiles Can Be Applied



In addition to network policy compliance, CUBE SIP profiles can be used to resolve incompatibilities between SIP devices inside the enterprise network. These are some of the situations in which incompatibilities can arise:

- A device rejects an unknown header (value or parameter) instead of ignoring it.
- A device sends incorrect data in a SIP message.
- A device does not implement (or implements incorrectly) protocol procedures.
- A device expects an optional header value or parameter, or an optional protocol procedure that can be implemented in multiple ways.
- A device sends a value or parameter that must be changed or suppressed before it leaves or enters the network.
- Variations in the SIP standards on how to achieve certain functions.

The SIP profiles feature on CUBE provides a solution to these incompatibilities and customization issues.

SIP profiles can also be used to change a header name from the long form to the compact form. For example, From to f. This can be used as a way to reduce the length of a SIP message. By default, the device never sends the compact form of the SIP messages although it receives either the long or the short form.

Feature Information

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 43: Feature Information for SIP Profiles

Feature Name	Releases	Feature Information
SIP Profiles (for inbound messages)	Baseline Functionality	This feature modifies the following commands: The inbound keyword was added to the sip-profiles and voice-class sip profiles commands.

Important Characteristics of SIP Profiles

Given below are a few important notes for SIP Profiles:

- Session Initiation Protocol (SIP) and Session Description Protocol (SDP) headers are supported. SDP can be either a standalone body or part of a Multipurpose Internet Mail Extensions (MIME) message.
- The rules that are configured for an INVITE message are applied only to the first INVITE of a call. A special REINVITE keyword is used to manipulate subsequent INVITEs of a call.
- Manipulation of SIP headers by outbound SIP profiles occurs as the last step before the message leaves the CUBE device; that is, after destination dial-peer matching has taken place. Changes to the SIP messages are not remembered or acted on by the CUBE application. The Content-length field is recalculated after the SIP Profiles rules are applied to the outgoing message.
- If the **ANY** keyword is used in place of a header, it indicates that a rule must be applied to any message within the specified category.
- SIP header modification can be cryptic. It can sometimes be easier to remove a header and add it back (with the new value), rather than modifying it.
- To include "?" (question-mark) character as part of match-pattern or replace-pattern, you must press "Ctrl+v" keys and then type "?". This is needed to treat "?" as an input character itself instead of usual device help prompt.



Note Regex features like look-ahead, look-behind, operator, and non capturing group are not supported (for example, `?!`, `?:`, `?<=,`, and `so| on`).

- For header values used to add, modify or copy a header:
 - If a whitespace occurs, the entire value must be included between double quotes. For example, "User-Agent: CISCO CUBE"
 - If double quotes occur, a back slash must prefix the double quotes. For example, "User-Agent: \"CISCO\" CUBE"
 - Basic regular expressions are supported.
- If an incoming SIP message contains certain proprietary attributes, CUBE can copy these unsupported SDP attributes or lines from incoming leg to outgoing leg using a SIP profile rule.
- The copy variable can be used in an outbound profile to add or modify the outgoing message.
- Copy Variables u01 to u99 are shared by inbound and outbound SIP Profiles.

Inbound SIP Profile:

- If the incoming message contains multiple instances of the same header, the header values are stored as a comma separated list, and this needs to be considered while modifying it.
- Modification by an inbound SIP profile takes place before regular SIP call processing happens so that behavior of CUBE would be as if it received the message directly without modification.

If inbound dial peer matching fails as required information could not be extracted from headers (like Request-URI, Via, From or To) due to issues in them, global level sip-profile config is applied. An example is a request with invalid SIP-Req-URI.

- After modification by inbound SIP Profiles, the parameters in SIP message might change, which might change the inbound dial-peer matched when actual dial-peer lookup is done.
- In the register pass-through feature, there is only one dial-peer for register and response. So both register from phone and response from registrar would go through the same inbound sip profile under the dial-peer if any.

Restrictions

- Removal or addition of mandatory headers is not supported. You can only modify mandatory headers. Mandatory SIP headers include To, From, Via, CSeq, Call-Id, and Max-Forwards. Mandatory SDP headers include v, o, s, t, c, and m.
- Addition or removal of entire Multipurpose Internet Mail Extensions (MIME) or (Session Description Protocol) SDP bodies from SIP messages is not supported.
- Syntax checking is not performed on SIP messages after SIP profile rules have been applied. Changes that are specified in the SIP profile should result in valid SIP protocol exchanges.
- The header length (including header name) after modification should not exceed 300 characters. Max header length for add value is approximately 220 characters. Max SDP length is 2048 characters. If any header length exceeds this maximum value after applying SIP profiles, then the profile is not applied.
- If a header-name is changed to its compact form, further SIP profile rules cannot be applied on that header. Thus a SIP profile rule modifying a header name to its compact form must be the last rule on that header.
- The "image" m-line attributes (m=image 16850 udptl t38) cannot be modified using SIP profiles. SIP profiles can be applied only on audio and video m-lines in SDP.
- In a high-availability (HA) scenario, SIP profiles copy variable data is not check-pointed to standby.
- Limitations and restrictions of outbound SIP profiles apply to inbound SIP profiles as well.
- You cannot configure more than 99 variables for the SIP profiles copy option.
- Once a SIP profile is configured using rule tag, you cannot add rules without tags in the same profile and conversely.
- If a SIP profile is applied to modify the SDP content of a SIP message, CUBE does not increment the "o=" line version, which may cause ITSPs to disconnect the call. CUBE does not store the modified SDP after the application of the SIP profile.

Note that manipulation of SIP messages by outbound SIP profiles occurs as the final step before the outgoing message leaves the CUBE device, and occurs after destination dial-peer matching has taken place. Changes to SIP messages are not remembered or acted on by CUBE. The Content-length field is recalculated after SIP Profile rules are applied to outgoing messages.

How to Configure SIP Profiles

To use SIP Profiles, you must first configure the profile, then apply it either at the global (all dial-peers), tenant, or dial-peer levels. After a SIP profile is configured, it can be applied as an inbound or outbound profile.

Configure SIP Profile Rules Using Rule Tags

Configuring SIP profile rules using rule tags, allows you to perform the following tasks:

- Add a new rule at a chosen position without having to replace the whole profile.
- Modify a specific rule by specifying its rule tag.
- Remove a rule by specifying only its rule tag.

Below are the rule tag behaviors that must be considered while using rule tags in a SIP profile configuration:

- If a rule is added with the tag of an existing rule, then the existing rule is overwritten with the new rule.
- For inserting a rule at the desired position, the SIP profile configuration should be in rule format. In case the SIP profile is in nonrule format, upgrade the SIP profiles to rule format before inserting a rule.
- If a new rule is inserted, the new rule takes the position that is specified in **before tag**. The subsequent rules are incremented sequentially.

For example:

```
rule before 10 request INVITE sip-header From modify "(<.*:)(.*@)" "\1gateway@"
```

- When a rule is removed, the tags that are associated with the subsequent rules remain unchanged.
- If a rule is added to a vacant tag, the new rule gets associated with the vacant tag and the subsequent rules remain unchanged.

Upgrade or Downgrade SIP Profile Configurations

You can upgrade SIP profile rules to include rule tags or downgrade to remove them.

SUMMARY STEPS

1. **enable**
2. Enter the following to upgrade SIP profiles configurations to rule-format:
 - **voice sip sip-profiles upgrade**
3. Enter the following to downgrade SIP profiles configurations to non-rule format:
 - **voice sip sip-profiles downgrade**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	Enter the following to upgrade SIP profiles configurations to rule-format: <ul style="list-style-type: none"> • voice sip sip-profiles upgrade Example: In EXEC(#) mode: Device# voice sip sip-profiles upgrade	Upgrades all SIP Profiles to rule-format configurations.
Step 3	Enter the following to downgrade SIP profiles configurations to non-rule format: <ul style="list-style-type: none"> • voice sip sip-profiles downgrade Example: In EXEC(#) mode: Device# voice sip sip-profiles downgrade	Downgrades all SIP Profiles from rule-format configurations to non-rule format configurations.
Step 4	end	Exits privileged EXEC mode.

What to do next

Now apply the SIP Profile as an inbound or outbound SIP profile.

Configure a SIP Profile to Manipulate SIP Request or Response Headers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-profiles** *profile-id*
4. Enter one of the following to add, remove, modify SIP headers:
 - [rule *x*] **request message** {**sip-header** | **sdp-header**} *header-to-add* **add** *header-value-to-add*
 - [rule *x*] **request message** {**sip-header** | **sdp-header**} *header-to-remove* **remove**
 - [rule *x*] **request message** {**sip-header** | **sdp-header**} *header-to-modify* **modify** *header-value-to-match* *header-value-to-replace*
5. Enter one of the following to add, remove, or modify SIP response headers:
 - [rule *x*] **response message** [**method** *method-type*] {**sip-header** | **sdp-header**} *header-to-add* **add** *header-value-to-add*
 - [rule *x*] **response message** [**method** *method-type*] {**sip-header** | **sdp-header**} *header-to-remove* **remove**

- [rule x] **response message** [method method-type] {sip-header | sdp-header} header-to-modify **modify** header-value-to-match header-value-to-replace

6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	voice class sip-profiles profile-id Example: Device(config)# voice class sip-profiles 10	Creates a SIP Profile and enters voice class configuration mode.
Step 4	Enter one of the following to add, remove, modify SIP headers: <ul style="list-style-type: none"> • [rule x] request message {sip-header sdp-header} header-to-add add header-value-to-add • [rule x] request message {sip-header sdp-header} header-to-remove remove • [rule x] request message {sip-header sdp-header} header-to-modify modify header-value-to-match header-value-to-replace 	According to your choice, this step does one of the following: <ul style="list-style-type: none"> • Adds a SIP or SDP header to a SIP request. • Removes a SIP or SDP header from a SIP request. • Modifies a SIP or SDP header in a SIP request. • If the ANY is used, the rule is applied to the specified header when it appears in any message type. • When specifying a profile rule header value: <ul style="list-style-type: none"> • If a value includes a space, the entire value must be included between double quotes. For example, “User-Agent: CISCO CUBE” • When using double quotes in a value, delimit with a backslash. • Simple regular expressions are supported.
Step 5	Enter one of the following to add, remove, or modify SIP response headers: <ul style="list-style-type: none"> • [rule x] response message [method method-type] {sip-header sdp-header} header-to-add add header-value-to-add • [rule x] response message [method method-type] {sip-header sdp-header} header-to-remove remove • [rule x] response message [method method-type] {sip-header sdp-header} header-to-modify modify header-value-to-match header-value-to-replace 	According to your choice, this step does one of the following: <ul style="list-style-type: none"> • Adds a SIP or SDP header to a SIP response. • Removes a SIP or SDP header from a SIP response. • Modifies a SIP or SDP header in a SIP response. • All notes in the previous step are applicable here.

	Command or Action	Purpose
Step 6	end	Exits to privileged EXEC mode

Processing Unsupported SDP Headers

To modify SDP headers that CUBE is not natively aware of, first configure SDP pass-through and then make the necessary modifications through the outbound dial-peer.

1. Configure CUBE to pass-through custom SDP on in-leg.
2. Define rule to **Copy** relevant attributes from peer SDP on out leg.
3. Define rule to **Add** or **Modify** attributes in outbound SDP with copied data.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. To enable copying of unsupported SDP attribute from incoming leg to outbound leg, you must enable one of the following commands:
 - In Global VoIP SIP configuration mode


```
pass-thru content custom-sdp
```
 - In dial-peer configuration mode (The configuration is applied on the incoming dial-peer)


```
voice-class sip pass-thru content custom-sdp
```
4. **voice class sip-profiles** *profile-id*
5. Enter one of the following to copy an unsupported SDP line or attribute from peer leg's SDP and add, modify, or remove in the outgoing SDP:
 - [rule *x*] {**request/response**} ANY **peer-header** **sdm** **mline-index** *index* **COPY** *match-pattern* *copy-variable*
 - [rule *x*] {**request/response**} ANY **sdm** **header** **mline-index** *indexheader-name* **ADD** *copy-variable*
 - [rule *x*] {**request/response**} ANY **sdm** **header** **mline-index** *indexheader-name* **MODIFY** *copy-variable* + *replace-pattern*
 - [rule *x*] { **request/response**} ANY **sdm** **header** **mline-index** *indexheader-name* **REMOVE**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
Step 3	<p>To enable copying of unsupported SDP attribute from incoming leg to outbound leg, you must enable one of the following commands:</p> <ul style="list-style-type: none"> In Global VoIP SIP configuration mode pass-thru content custom-sdp In dial-peer configuration mode (The configuration is applied on the incoming dial-peer) voice-class sip pass-thru content custom-sdp <p>Example:</p> <p>In Global VoIP SIP configuration mode:</p> <pre>Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# pass-thru content custom-sdp</pre> <p>Example:</p> <p>In Dial-peer configuration mode:</p> <pre>Device(config)# dial-peer voice 2 voip Device(config-dial-peer)# voice-class sip pass-thru content custom-sdp</pre>	<p>Enables copying of unsupported SDP attributes per m-line to the peer leg so that it can be used in outgoing SIP messages.</p> <p>Note Enabling this command does not enable the SDP Passthrough feature.</p>
Step 4	<p>voice class sip-profiles <i>profile-id</i></p> <p>Example:</p> <pre>Device(config)# voice class sip-profiles 10</pre>	<p>Voice class sip-profile is configured on the outbound dial-peer or as a global configuration.</p> <p>Creates a SIP Profile and enters voice class configuration mode.</p>
Step 5	<p>Enter one of the following to copy an unsupported SDP line or attribute from peer leg's SDP and add, modify, or remove in the outgoing SDP:</p> <ul style="list-style-type: none"> [rule <i>x</i>] {request/response} ANY peer-header sdp mline-index <i>index</i> COPY <i>match-pattern copy-variable</i> [rule <i>x</i>] {request/response} ANY sdp-header mline-index <i>indexheader-name</i> ADD <i>copy-variable</i> [rule <i>x</i>] {request/response} ANY sdp-header mline-index <i>indexheader-name</i> MODIFY <i>copy-variable + replace-pattern</i> [rule <i>x</i>] { request/response} ANY sdp-header mline-index <i>indexheader-name</i> REMOVE 	<p>M-line Index values:</p> <ul style="list-style-type: none"> 0 - A value of zero represents the session level. 1–6 - A value in the range of one to six represents the m-line number in SDP. <p>Copy: Enables copying of SDP line or attribute from peer leg SDP.</p> <p>Add: Enables adding the copied SDP line or attribute in the outgoing SDP.</p> <p>Modify: Enables modifying SDP line or attribute in the outgoing SDP.</p> <p>Remove: Enables removing SDP line or attribute in the outgoing SDP.</p>
Step 6	end	Exits to privileged EXEC mode.

Example: Configuring SIP Profile Rules (Attribute Passing)

```
rule 10 response ANY peer-header sdp mline-index 4 copy "(a=ixmap:0.*)" u01
rule 20 response ANY sdp-header mline-index 4 a=ixmap add "\u01"
```

Example: Configuring SIP Profile Rules (Parameter Passing)

```
rule 30 response ANY peer-header sdp mline-index 2 copy "a=fmtp:126.*(max-fps=...)" u04
rule 40 response ANY sdp-header mline-index 2 a=fmtp:126 modify ";" "\u04;"
```

Example: Configuration to Remove an Attribute

```
rule 50 response ANY sdp-header mline-index 4 a=test REMOVE
```

Use Non-standard SIP Headers in SIP Profiles

In addition to the standard set of headers available when creating SIP profile rules, it is possible to carry out a similar set of functions for any other non-standard header.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-profiles** *profile-id*
4. Enter one of the following to add, copy, remove, or modify non-standard SIP request headers:
 - [rule *x*] **request message sip-header non-standard-header-to-add add**
non-standard-header-value-to-add
 - [rule *x*] **request message sip-header non-standard-header-to-copy copy**
non-standard-header-value-to-match copy-variable
 - [rule *x*] **request message sip-header non-standard-header-to-remove remove**]
 - [rule *x*] **request message {sip-header } non-standard-header-to-modify modify**
non-standard-header-value-to-match non-standard-header-value-to-replace
5. Enter one of the following to add, copy, remove, or modify non-standard SIP response headers:
 - [rule *x*] **response message [method method-type] sip-header non-standard-header-to-add add**
non-standard-header-value-to-add
 - [rule *x*] **response message [method method-type] sip-header non-standard-header-to-copy copy**
non-standard-header-value-to-match copy-variable
 - [rule *x*] **response message [method method-type] sip-header non-standard-header-to-remove remove**
 - [rule *x*] **response message [method method-type] sip-header non-standard-header-to-modify modify**
non-standard-header-value-to-match non-standard-header-value-to-replace
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	voice class sip-profiles <i>profile-id</i> Example: Device(config)# voice class sip-profiles 10	Creates a SIP Profiles and enters voice class configuration mode.
Step 4	Enter one of the following to add, copy, remove, or modify non-standard SIP request headers: <ul style="list-style-type: none"> • [rule <i>x</i>] request message sip-header <i>non-standard-header-to-add</i> add <i>non-standard-header-value-to-add</i> • [rule <i>x</i>] request message sip-header <i>non-standard-header-to-copy</i> copy <i>non-standard-header-value-to-match</i> <i>copy-variable</i> • [rule <i>x</i>] request message sip-header <i>non-standard-header-to-remove</i> remove] • [rule <i>x</i>] request message {sip-header } <i>non-standard-header-to-modify</i> modify <i>non-standard-header-value-to-match</i> <i>non-standard-header-value-to-replace</i> 	According to your choice, this step does one of the following: <ul style="list-style-type: none"> • Adds a non-standard SIP header to a SIP request. • Copies a non-standard SIP header value to a copy variable. • Removes a non-standard SIP header from a SIP request. • Modifies a non-standard SIP header in a SIP request. • If the ANY message keyword is used, the rule is applied to the specified header when it appears in any message type. • For <i>non-standard-header-value-to-add</i> used to add a non-standard header, <i>non-standard-header-value-to-match</i> or <i>non-standard-header-value-to-replace</i> used to modify a non-standard header when specifying a profile rule header value: <ul style="list-style-type: none"> • If a value includes a space , the entire value must be included between double quotes. For example, “User-Agent: CISCO CUBE” • When using double quotes in a value, delimit with a backslash. • Simple regular expressions are supported.
Step 5	Enter one of the following to add, copy, remove, or modify non-standard SIP response headers: <ul style="list-style-type: none"> • [rule <i>x</i>] response message [method <i>method-type</i> sip-header <i>non-standard-header-to-add</i> add <i>non-standard-header-value-to-add</i> 	According to your choice, this step does one of the following: <ul style="list-style-type: none"> • Adds a non-standard header to a SIP response message. • Copies contents from a non-standard SIP header to a SIP response.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • [rule x] response message [method method-type] sip-header non-standard-header-to-copy copy non-standard-header-value-to-match copy-variable • [rule x] response message [method method-type] sip-header non-standard-header-to-remove remove • [rule x] response message [method method-type] sip-header non-standard-header-to-modify modify non-standard-header-value-to-match non-standard-header-value-to-replace 	<ul style="list-style-type: none"> • Removes a non-standard header to a SIP response. • Modifies a non-standard SIP header in a SIP response. • All notes from the previous step are applicable here.
Step 6	end	Exits to privileged EXEC mode

Configure a SIP Profile as an Outbound Profile

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Apply the SIP profile to a dial peer:
 - **voice-class sip profiles** *profile-id* in the dial-peer configuration mode.
 - **sip-profiles** *profile-id* in the global VoIP configuration mode
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	Apply the SIP profile to a dial peer: <ul style="list-style-type: none"> • voice-class sip profiles <i>profile-id</i> in the dial-peer configuration mode. • sip-profiles <i>profile-id</i> in the global VoIP configuration mode <p>Example: In dial-peer configuration mode</p> <pre>!Applying SIP profiles to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip profiles 30 Device (config-dial-peer)# end</pre>	

	Command or Action	Purpose
	Example: In global VoIP SIP mode <pre>! Applying SIP profiles globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# sip-profiles 20 Device (config-voi-sip)# end</pre>	
Step 4	end	Exits to privileged EXEC mode .

Configure a SIP Profile as an Inbound Profile

You can configure a SIP profile as an inbound profile applied globally or to multiple inbound dial peers. Inbound SIP profiles feature must be enabled before applying it.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **sip-profiles inbound**
6. Apply the SIP profile to a dial peer:
 - **voice-class sip profiles *profile-id* inbound** in the dial-peer configuration mode.
 - **sip-profiles *profile-id* inbound** in the global VoIP configuration mode
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters global VoIP configuration mode.
Step 4	sip Example: <pre>Device(config-voi-serv)# sip</pre>	Enters global VoIP SIP configuration mode.

	Command or Action	Purpose
Step 5	sip-profiles inbound Example: <pre>Device(config-voi-sip)# sip-profiles inbound</pre>	Enables inbound SIP profiles feature.
Step 6	Apply the SIP profile to a dial peer: <ul style="list-style-type: none"> • voice-class sip profiles <i>profile-id</i> inbound in the dial-peer configuration mode. • sip-profiles <i>profile-id</i> inbound in the global VoIP configuration mode Example: In dial-peer configuration mode <pre>!Applying SIP profiles to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip profiles 30 inbound Device (config-dial-peer)# end</pre> Example: In global VoIP SIP mode <pre>! Applying SIP profiles globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# sip-profiles 20 inbound Device (config-voi-sip)# end</pre>	
Step 7	end	Exits to privileged EXEC mode

Supported SIP Messages

This section provides the CLI options of the SIP messages that you can process with the CUBE SIP profiles feature.

SIP Requests

Supported SIP requests are the following:

```
ACK          sip ack
ANY          any sip request
BYE         sip bye
CANCEL      sip cancel
COMET       sip comet
INFO        sip info
INVITE      sip invite
NOTIFY      sip notify
OPTIONS     sip options
PRACK       sip prack
PUBLISH     sip publish
```

```
REFER      sip refer
REGISTER   sip register
REINVITE   sip reinvite
SUBSCRIBE  sip subscribe
UPDATE     sip info
```

SIP Responses

Supported SIP responses are the following:

```
100 Response code 100
180 Response code 180
181 Response code 181
182 Response code 182
183 Response code 183
200 Response code 200
202 Response code 202
300 Response code 300
301 Response code 301
302 Response code 302
305 Response code 305
380 Response code 380
400 Response code 400
401 Response code 401
402 Response code 402
403 Response code 403
404 Response code 404
405 Response code 405
406 Response code 406
407 Response code 407
408 Response code 408
409 Response code 409
410 Response code 410
412 Response code 412
413 Response code 413
414 Response code 414
415 Response code 415
416 Response code 416
417 Response code 417
420 Response code 420
421 Response code 421
422 Response code 422
423 Response code 423
480 Response code 480
481 Response code 481
482 Response code 482
483 Response code 483
484 Response code 484
485 Response code 485
486 Response code 486
487 Response code 487
488 Response code 488
489 Response code 489
491 Response code 491
493 Response code 493
500 Response code 500
501 Response code 501
502 Response code 502
503 Response code 503
504 Response code 504
505 Response code 505
513 Response code 513
580 Response code 580
600 Response code 600
```

603 Response code 603
 604 Response code 604
 606 Response code 606
 ANY Any Response

SIP Headers

Supported SIP headers are the following:



Note Non-standard SIP headers are also supported.

Accept-Contact	SIP header	Accept-Contact
Accept-Encoding	SIP header	Accept-Encoding
Accept-Header	SIP header	Accept
Accept-Language	SIP header	Accept-Language
Accept-Resource-Priority	SIP header	Accept-Resource-Priority
Alert-Info	SIP header	Alert-Info
Allow-Events	SIP header	Allow-Events
Allow-Header	SIP header	Allow
Also	SIP header	Also
Authorization	SIP header	Authorization
CC-Diversion	SIP header	CC-Diversion
CC-Redirect	SIP header	CC-Redirect
CSeq	SIP header	CSeq
Call-ID	SIP header	Call-ID
Call-Info	SIP header	Call-Info
Cisco-Gcid	SIP header	Cisco-Gcid
Cisco-Guid	SIP header	Cisco-Guid
Contact	SIP header	contact
Content-Disposition	SIP header	Content-Disposition
Content-Encoding	SIP header	Content-Encoding
Content-Id	SIP header	Content-Id
Content-Length	SIP header	Content-Length
Content-Type	SIP header	Content-Type
Date	SIP header	Date
Diversion	SIP header	Diversion
Event	SIP header	Event
Expires	SIP header	Expires
From	SIP header	FROM
History-Info	SIP header	History-Info
Location	SIP header	Location
MIME-Version	SIP header	MIME-Version
Max-Forwards	SIP header	Max-Forwards
Min-Expires	SIP header	Min-Expires
Min-SE	SIP header	Min-SE
Orig-dial-plan	SIP header	Orig-dial-plan
P-Asserted-Identity	SIP header	P-Asserted-Identity
P-Preferred-Identity	SIP header	P-Preferred-Identity
P-RTP-Stat	SIP Header	P-RTP-Stat
Privacy	SIP header	Privacy
Proxy-Authenticate	SIP header	Proxy-Authenticate
Proxy-Authorization	SIP header	Proxy-Authorization
Proxy-Require	SIP header	Proxy-Require
Rack	SIP header	Rack
Reason	SIP header	Reason
Record-Route	SIP header	Record-Route
Refer-To	SIP header	Refer-To
Referred-By	SIP header	Referred-By
Reject-Contact	SIP header	Reject-Contact

Remote-Party-ID	SIP header Remote-Party-ID
Replaces	SIP header Replaces
Request-Disposition	SIP header Request-Disposition
Requested-By	SIP header Requested-By
Require	SIP header Require
Resource-Priority	SIP header Resource-Priority
Retry-After	SIP header Retry-After
Route	SIP header Route
Rseq	SIP header Rseq
SIP-ETag	SIP header SIP-ETag
SIP-If-Match	SIP header SIP-If-Match
SIP-Req-URI	SIP Request URI
SIP-StatusLine	SIP Status-Line
Server	SIP header Server
Session-Expires	SIP header Session-Expires
Session-Header	SIP header Session
Session-ID	SIP header Session ID
Subscription-State	SIP header Subscription-State
Supported	SIP header Supported
Term-dial-plan	SIP header Term-dial-plan
Timestamp	SIP header Timestamp
To	SIP header TO
Unsupported	SIP header Unsupported
User-Agent	SIP header User-Agent
Via	SIP header Via
WORD	Any other SIP header name
WWW-Authenticate	SIP header WWW-Authenticate
Warning	SIP header Warning

SDP Headers

Supported SDP headers are the following:

Attribute	SDP header Attribute
Audio-Attribute	SDP Audio Attribute
Audio-Bandwidth-Info	SDP Audio Bandwidth Info
Audio-Connection-Info	SDP Audio Connection Info
Audio-Encryption-Key	SDP Audio Encrypt key
Audio-Media	SDP Audio Media
Audio-Session-Info	SDP Audio Session Info
Bandwidth-Key	SDP header Bandwidth-Key
Connection-Info	SDP header Connection-Info
Email-Address	SDP header Email-Address
Encrypt-Key	SDP header Encrypt-Key
Phone-Number	SDP header Phone-Number
Repeat-Times	SDP header Repeat-Times
Session-Info	SDP header Session-info
Session-Name	SDP header Session-Name
Session-Owner	SDP header Session
Time-Adjust-Key	SDP header Time-Adjust-Key
Time-Header	SDP header Time
Url-Descriptor	SDP header Url-Descriptor
Version	SDP Version
Video-Attribute	SDP Video Attribute
Video-Bandwidth-Info	SDP Video Bandwidth Info
Video-Connection-Info	SDP Video Connection Info
Video-Encryption-Key	SDP Video Encryption Key
Video-Media	SDP Video Media
Video-Session-Info	SDP Video Session Info
mline-index	M-Line index for SDP Line

Verify SIP Profiles

SUMMARY STEPS

1. `show dial-peer voice id | include profile`

DETAILED STEPS

`show dial-peer voice id | include profile`

Displays information related to SIP profiles configured on the specified dial peer.

Example:

```
Device# show dial-peer voice 10 | include sip profile
voice class sip profiles = 11
voice class sip profiles inbound = 10
```

Troubleshoot SIP Profiles

SUMMARY STEPS

1. `debug ccsip all`

DETAILED STEPS

The following debugs can also be used:

- `debug ccsip info`
- `debug ccsip feature sip-profiles`
- `debug ccsip error`

`debug ccsip all`

This command displays the applied SIP profiles.

Example:

Applied SIP profile is highlighted in the example below.

```
Device# debug ccsip all
...
Oct 12 06:51:53.619: //-1/735085DC8F3D/SIP/Info/sipSPIGetShrlPeer:
Try match incoming dialpeer for Calling number:
: sippOct 12 06:51:53.619:
//-1/735085DC8F3D/SIP/Info/sipSPIGetCallConfig:
Peer tag 2 matched for incoming call
```



```

Oct 12 06:51:53.619: //-1/xxxxxxxxxxxx/SIP/Info/sipSPIGetCallConfig:
      voice class SIP profiles tag is set : 1
Oct 12 06:51:53.619: //-1/735085DC8F3D/SIP/Info/sipSPIGetCallConfig:
      Not using Voice Class Codec
Oct 12 06:51:53.619: //-1/735085DC8F3D/SIP/Info/sipSPIGetCallConfig:
      xcoder high-density disabled
Oct 12 06:51:53.619: //-1/735085DC8F3D/SIP/Info/sipSPIGetCallConfig:
      Flow Mode set to FLOW_THROUGH

```

This command also displays the modifications that are performed by the SIP profile configuration, by preceding the modification information with the word `sip_profiles`, as highlighted in the following example.

Example:

```

Device# debug ccsip all
...
Oct 12 06:51:53.647: //-1/xxxxxxxxxxxx/SIP/Info/
sip_profiles_application_change_sdp_line:
New SDP header is added : b=AS: 1600
Oct 12 06:51:53.647: //-1/xxxxxxxxxxxx/SIP/Info/
sip_profiles_update_content_length:
Content length header before modification :
Content-Length: 290
Oct 12 06:51:53.647: //-1/xxxxxxxxxxxx/SIP/Info/
sip_profiles_update_content_length:
Content length header after modification :
Content-Length: 279

```

Examples: Adding, Modifying, Removing SIP Profiles

Example: Adding a SIP, SDP, or Peer Header

Example: Adding "b=AS:4000" SDP header to the video-media Header of the INVITE SDP Request Messages

```

Device(config)# voice class sip-profiles 10
Device(config-class)# request INVITE sdp-header Video-Bandwidth-Info add "b=AS:4000"
Device(config-class)# end

```

Example: Adding "b=AS:4000" SDP header to the video-media Header of the INVITE SDP Request Messages in rule format

```

Device(config)# voice class sip-profiles 10
Device(config-class)# rule 1 request INVITE sdp-header Video-Bandwidth-Info add "b=AS:4000"
Device(config-class)# end

```

Example: Adding the Retry-After Header to the SIP 480 Response Messages

```

Device(config)# voice class sip-profiles 20

```

Example: Modifying a SIP, SDP, or Peer Header

```
Device(config-class)# response 480 sip-header Retry-After add "Retry-After: 60"
Device(config-class)# end
```

Example: Adding the Retry-After Header to the SIP 480 Response Messages in rule format

```
Device(config)# voice class sip-profiles 20
Device(config-class)# rule 1 response 480 sip-header Retry-After add "Retry-After: 60"
Device(config-class)# end
```

Example: Adding "User-Agent: SIP-GW-UA" to the User-Agent Field of the 200 Response SIP Messages

```
Device(config)# voice class sip-profiles 40
Device(config-class)# response 200 sip-header User-Agent add "User-Agent: SIP-GW-UA"
Device(config-class)# end
```

Example: Adding "User-Agent: SIP-GW-UA" to the User-Agent Field of the 200 Response SIP Messages in rule format

```
Device(config)# voice class sip-profiles 40
Device(config-class)# rule 1 response 200 sip-header User-Agent add "User-Agent: SIP-GW-UA"
Device(config-class)# end
```

Example: Adding "a=ixmap:0 ping" in M-Line number 4 of the INVITE SDP Request Messages

```
Device(config)# voice class sip-profiles 10
Device(config-class)# request INVITE sdp-header mline-index 4 a=ixmap add "a=ixmap:0 ping"
Device(config-class)# end
```

Example: Modifying a SIP, SDP, or Peer Header

Example: Modifying SIP-Req-URI of the Header of the INVITE and RE-INVITE SIP Request Messages to include "user=phone"

```
Device(config)# voice class sip-profiles 30
Device(config-class)# request INVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
Device(config-class)# request RE-INVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
Device(config-class)# end
```

Example: Modifying SIP-Req-URI of the Header of the INVITE and RE-INVITE SIP Request Messages to include "user=phone" in rule format

```
Device(config)# voice class sip-profiles 30
```

```
Device(config-class)# rule 1 request INVITE sip-header SIP-Req-URI modify "; SIP/2.0"
";user=phone SIP/2.0"
Device(config-class)# rule 2 request RE-INVITE sip-header SIP-Req-URI modify "; SIP/2.0"
";user=phone SIP/2.0"
Device(config-class)# end
```

Modify the From Field of a SIP INVITE Request Messages to "gateway@gw-ip-address" Format

For example, modify 2222000020@10.13.24.7 to gateway@10.13.24.7

```
Device(config)# voice class sip-profiles 20
Device(config-class)# request INVITE sip-header From modify "<.*> (.*)" "\1gateway@"
```

Modify the From Field of a SIP INVITE Request Messages to "gateway@gw-ip-address" Format in rule format

For example, modify 2222000020@10.13.24.7 to gateway@10.13.24.7

```
Device(config)# voice class sip-profiles 20
Device(config-class)# rule 1 request INVITE sip-header From modify "<.*> (.*)" "\1gateway@"
```

Replace "CiscoSystems-SIP-GW-UserAgent" with "-" in the Originator Header of the SDP in INVITE Request Messages

```
Device(config)# voice class sip-profiles 10
Device(config-class)# request INVITE sdp-header Session-Owner modify
"CiscoSystems-SIP-GW-UserAgent" "-"
```

Replace "CiscoSystems-SIP-GW-UserAgent" with "-" in the Originator Header of the SDP in INVITE Request Messages in rule format

```
Device(config)# voice class sip-profiles 10
Device(config-class)# rule 1 request INVITE sdp-header Session-Owner modify
"CiscoSystems-SIP-GW-UserAgent" "-"
```

Convert "sip uri" to "tel uri" in Req-URI, From and To Headers of SIP INVITE Request Messages

For example, modify sip:2222000020@9.13.24.6:5060" to "tel:2222000020

```
Device(config)# voice class sip-profiles 40
Device(config-class)# request INVITE sip-header SIP-Req-URI modify "sip:(.*)@[^ ]+" "tel:\1"
Device(config-class)# request INVITE sip-header From modify "<sip:(.*)@.*>" "<tel:\1>"
Device(config-class)# request INVITE sip-header To modify "<sip:(.*)@.*>" "<tel:\1>"
```

Convert "sip uri" to "tel uri" in Req-URI, From and To Headers of SIP INVITE Request Messages in rule format

For example, modify sip:2222000020@9.13.24.6:5060" to "tel:2222000020

```
Device(config)# voice class sip-profiles 40
Device(config-class)# rule 1 request INVITE sip-header SIP-Req-URI modify "sip:(.*)@[^ ]+"
"tel:\1"
```

Example: Modifying a SIP, SDP, or Peer Header

```
Device(config-class)# rule 2 request INVITE sip-header From modify "<sip:(.*)@.*>" "<tel:\1>"
Device(config-class)# rule 3 request INVITE sip-header To modify "<sip:(.*)@.*>" "<tel:\1>"
```

Example: Change the Audio Attribute Ptime:20 to Ptime:30

Inbound ptime:

```
a=ptime:20
```

Outbound ptime:

```
a=ptime:30
```

```
Device(config)# voice class sip-profiles 103
```

```
Device(config-class)# request ANY sdp-header Audio-Attribute modify "a=ptime:20" "a=ptime:30"
```

Example: Modify Audio direction "Audio-Attribute"

Some service providers or customer equipment reply to delay offer invites and or re-invites that contain a=inactive with a=inactive, a=recvonly, or a=sendonly. This can create an issue when trying to transfer or retrieve a call from hold. The result is normally one-way audio after hold or resume or transfer or moh is not heard. To resolve this issue changing the audio attribute to Sendrecv prevents the provider from replaying back with a=inactive, a=recvonly, or a=sendonly.

Case 1:

Inbound Audio-Attribute

```
a=inactive
```

Outbound Audio-Attribute

```
a=sendrecv
```

Case 2:

Inbound Audio-Attribute

```
a=recvonly
```

Outbound Audio-Attribute

```
a=sendrecv
```

Case 3

Inbound Audio-Attribute

```
a=sendonly
```

Outbound Audio-Attribute

```
a=sendrecv
```

```
Device(config)# voice class sip-profiles 104
```

```
Device(config-class)# request any sdp-header Audio-Attribute modify "a=inactive" "a=sendrecv"
```

```
Device(config-class)# request any sdp-header Audio-Attribute modify "a=recvonly" "a=sendrecv"
```

```
Device(config-class)# request any sdp-header Audio-Attribute modify "a=sendonly" "a=sendrecv"
```

```
Device(config-class)# response any sdp-header Audio-Attribute modify "a=inactive" "a=sendrecv"
```

```
Device(config-class)# response any sdp-header Audio-Attribute modify "a=recvonly" "a=sendrecv"
Device(config-class)# response any sdp-header Audio-Attribute modify "a=sendonly" "a=sendrecv"
```

Example: Modifying Packetization Mode in a=fmtp line of M-line number 2 of the INVITE SDP Request Messages

```
Device(config)# voice class sip-profiles 10
Device(config-class)# request INVITE sdp-header mline-index 2 a=fmtp modify
"packetization-mode=1" "packetization-mode=0"
Device(config-class)# end
```

Example: Remove a SIP, SDP, or Peer Header

Remove Cisco-Guid SIP header from all Requests and Responses

```
Device(config)# voice class sip-profiles 20
Device(config-class)# request ANY sip-header Cisco-Guid remove
Device(config-class)# response ANY sip-header Cisco-Guid remove
Device(config-class)# end
```

Remove Server Header from 100 and 180 SIP Response Messages

```
Device(config)# voice class sip-profiles 20
Device(config-class)# response 100 sip-header Server remove
Device(config-class)# response 180 sip-header Server remove
Device(config-class)# end
```

Removing a SIP Profile rule in rule format configuration

SIP Profile configuration in rule format

```
Device(config)# voice class sip-profiles 10
Device(config-class)# rule 1 request any sdp-header Audio-Attribute modify "a=inactive"
"a=sendrecv"
Device(config-class)# rule 2 request any sdp-header Audio-Attribute modify "a=recvonly"
"a=sendrecv"
Device(config-class)# end
```

Removing the rule using rule tag

```
Device(config)# voice class sip-profiles 10
Device(config-class)# no rule 1
Device(config-class)# end
```

Once the rule is removed, the tag belonging to the removed rule remains vacant. The tags associated with the subsequent rules are unchanged.

The SIP Profile configuration after removing the rule

```
Device(config)# voice class sip-profiles 10
Device(config-class)# rule 2 request any sdp-header Audio-Attribute modify "a=recvonly"
"a=sendrecv"
Device(config-class)# end
```

Example: Removing "a=ixmap" in M-Line number 4 of the INVITE SDP Request Messages

```
Device(config)# voice class sip-profiles 10
Device(config-class)# request INVITE sdp-header mline-index 4 a=ixmap REMOVE
Device(config-class)# end
```

Example: Inserting SIP Profile Rules

Example: Inserting a SIP Profile Rule

Inserting a SIP profile rule to a SIP Profile

```
Device(config)#voice class sip-profiles 1
Device(config-class)#rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
Device(config-class)#rule 2 request INVITE sip-header Supported Add "Supported: "
Device(config-class)#rule before 2 request INVITE sip-header To Modify "(.*)" "\1;temp=abc"
```

The SIP Profile after inserting the new rule

```
Device(config)#voice class sip-profiles 1
Device(config-class)#rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
Device(config-class)#rule 2 request INVITE sip-header To Modify "(.*)" "\1;temp=abc"
Device(config-class)#rule 3 request INVITE sip-header Supported Add "Supported: "
```

Example: Upgrading and Downgrading SIP Profiles automatically

Upgrading SIP Profiles to rule-format

The following is a snippet from **show running-config** command showing the SIP profiles in non-rule format:

```
Device#show running-config | section profiles 1
voice class sip-profiles 1
request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
request INVITE sip-header Supported Add "Supported: "
```

Execute the following command in EXEC (#) mode to upgrade the SIP Profiles to rule-format:

```
Device#voice sip sip-profiles upgrade
```

The following is a snippet from **show running-config** command showing the SIP profiles after upgrading to rule-format:

```
Device#show running-config | section profiles 1

voice class sip-profiles 1
  rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
  rule 2 request INVITE sip-header Supported Add "Supported: "
```

Downgrading SIP Profiles to non-rule format

The following is a snippet from **show running-config** command showing SIP profiles in rule-format:

```
Device#show running-config | section profiles 1

voice class sip-profiles 1
  rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
  rule 2 request INVITE sip-header Supported Add "Supported: "
```

Execute the following command in EXEC(#) mode to downgrade SIP Profiles to non-rule format:

```
Device# voice sip sip-profiles downgrade
```

The following is a snippet from **show running-config** command showing SIP profiles after downgrading to non-rule format:

```
Device#show running-config | section profiles 1

voice class sip-profiles 1
  request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
  request INVITE sip-header Supported Add "Supported: "
```

Example: Modifying Diversion Headers

Example: Modify Diversion Headers from Three-Digit Extensions to Ten Digits.

Most North American service providers require a ten digit diversion header. Prior to Call manager 8.6, Call manager would only send the extension in the diversion header. A SIP profile can be used to make the diversion header ten digits.

Call manager version 8.6 and above has the field "Redirecting Party Transformation CSS" which lets you expand the diversion header on the call manager.

The SIP profile will look for a diversion header containing "< sip:5..." , where ... stands for the three-digit extension and then concatenates 9789365 with these three digits.

Original Diversion Header:

```
Diversion:< sip:5100@161.44.77.193>;privacy=off;reason=unconditional;counter=1;screen=no
```

Modified Diversion Header:

```
Diversion: < sip:9789365100@10.86.176.19>;privacy=off;reason=unconditional;counter=1;screen=no
```

```
Device(config)# voice class sip-profiles 101
Device(config-class)# request Invite sip-header Diversion modify "< sip:5(...)"
"< sip:9789365\1@"
Device(config-class)# end
```

Example: Create a Diversion header depending on the area code in the From field

Most service providers require a redirected call to have a diversion header that contains a full 10 digit number that is associated with a SIP trunk group. Sometimes, a SIP trunk may cover several different area codes, states, and geographic locations. In this scenario, the service provider may require a specific number to be placed in the diversion header depending on the calling party number.

In the below example, if the From field has an area code of 978 "< sip:978", the SIP profile leaves the From field as is and adds a diversion header.

```
Device(config)# voice class sip-profiles 102
Device(config-class)# request INVITE sip-header From modify "From: (.*)< sip:978 (.*)@ (.*)"
"From:\1< sip:978\2@\3\x0ADiversion:
< sip:9789365000@10.86.176.19:5060;privacy=off;reason=unconditional;counter=1;screen=no"
```

The below diversion header is added. There was no diversion header before this was added:

```
Diversion: < sip:9789365000@10.86.176.19:5060;transport=udp>"
```

Example: Sample SIP Profile Application on SIP Invite Message

The SIP profile configured is below:

The SIP INVITE message before the SIP profile has been applied is show below:

```
voice class sip-profiles 1
  request INVITE sdp-header Audio-Bandwidth-Info add "b=AS:1600"
  request ANY sip-header Cisco-Guid remove
  request INVITE sdp-header Session-Owner modify "CiscoSystems-SIP-GW-UserAgent" "-"
```

```
INVITE sip:2222000020@9.13.40.250:5060 SIP/2.0
Via: SIP/2.0/UDP 9.13.40.249:5060;branch=z9hG4bK1A203F
From: "sipp " < sip:1111000010@9.13.40.249>;tag=F11AE0-1D8D
To: < sip:2222000020@9.13.40.250>
Date: Mon, 29 Oct 2007 19:02:04 GMT
Call-ID: 4561B116-858811DC-804DEF2E-4CF2D71B@9.13.40.249
Cisco-Guid: 1163870326-2240287196-2152197934-1290983195
Content-Length: 290
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 6906 8069 IN IP4 9.13.40.249
s=SIP Call
c=IN IP4 9.13.40.249
t=0 0
m=audio 17070 RTP/AVP 0
c=IN IP4 9.13.40.249
a=rtpmap:0 PCMU/8000
a=ptime:20
```

The SIP INVITE message after the SIP profile has been applied is shown below:

- The Cisco-Guid has been removed.
- CiscoSystemsSIP-GW-UserAgent has been replaced with -.
- The Audio-Bandwidth SDP header has been added with the value b=AS:1600.

```
INVITE sip:2222000020@9.13.40.250:5060 SIP/2.0
Via: SIP/2.0/UDP 9.13.40.249:5060;branch=z9hG4bK1A203F
```



```

From: "sipp " <sip:1111000010@9.13.40.249>;tag=F11AE0-1D8D
To: <sip:2222000020@9.13.40.250>
Date: Mon, 29 Oct 2007 19:02:04 GMT
Call-ID: 4561B116-858811DC-804DEF2E-4CF2D71B@9.13.40.249
Content-Length: 279

v=0
o=- 6906 8069 IN IP4 9.13.40.249
s=SIP Call
c=IN IP4 9.13.40.249
t=0 0
m=audio 17070 RTP/AVP 0
c=IN IP4 9.13.40.249
a=rtpmap:0 PCMU/8000
a=ptime:20
b=AS:1600

```

Example: Sample SIP Profile for Non-Standard SIP Headers

It is possible to add, copy, modify or delete any SIP header.

```

voice class sip-profiles 1
request INVITE sip-header X-Cisco-Recording-Participant copy "sip:(.*)@" u01
request INVITE sip-header X-Cisco-Recording-Participant modify "sip:sipp@" "sip:1000@"
request INVITE sip-header My-Info add "My-Info: MF Call"
request INVITE sip-header My-Info remove

```

Example: Copy User-to-User Information from REFER Message

When a call is transferred using REFER, user-to-user content from the originating message is not automatically copied to the triggered INVITE. This example illustrates how SIP profiles can be used to capture this information and pass it to the outbound INVITE, where it is added as a new header.

SIP profile 1210 applied to the incoming dial-peer copies the user-to-user information to a temporary header (x-user). This header is passed to the outbound leg where SIP profile 1211 extracts this information and uses it to create the new INVITE User-to-user header before removing the temporary x-user header.

To ensure that the x-user header is passed to the INVITE message, either use a sip-copylist that is applied to both dial-peers or enable unsupported header pass-through.

```

voice class sip-profiles 1210
request REFER sip-header Refer-To copy "Refer-To:.*User-to-User=(.*)>" u03
request REFER sip-header x-user add "x-user: TEST"
request REFER sip-header x-user modify "x-user: (.*)" "x-user: \u03"

voice class sip-profiles 1211
request INVITE sip-header x-user copy "x-user: (.*)" u05
request INVITE sip-header User-to-User add "User-to-User: TEST"
request INVITE sip-header User-to-User modify "User-to-User: (.*)" "User-to-User: \u05"
request INVITE sip-header x-user remove"

```




CHAPTER 28

Pass Unsupported SIP Headers

- [Overview, on page 273](#)
- [Supported SIP Headers, on page 274](#)
- [Unsupported Headers, on page 275](#)
- [Enable Configurable Pass-Through of SIP INVITE Parameters \(Global Level\), on page 275](#)
- [Enable Configurable Pass-Through of SIP INVITE Parameters \(Dial Peer Level\), on page 276](#)
- [Configure a Route String Header Pass-Through Using Pass-Through List, on page 278](#)
- [Example: Configuring a Route String Header Pass-Through Using Pass-Through List, on page 279](#)
- [Example: Passing a Header Not Supported by CUBE, on page 280](#)

Overview

This feature is used to pass parameters that are unsupported by Cisco Unified Border Element (CUBE), but mandatory to the service provider from one leg to another. When a SIP message is received, a check is done for the header, and if it is available, it is copied into a copy list and passed on to the outbound dial peer leg. The feature enables the Cisco Unified Border Element (Cisco UBE) platform to pass through end-to-end headers at a global or dial peer level that are not processed or understood in a Session Initiation Protocol (SIP) trunk to SIP trunk scenario.

Feature Information

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 44: Feature Information for Copying with SIP Profiles

Feature Name	Releases	Feature Information
Support for conditional header manipulation of SIP headers	Baseline Functionality	This feature modifies the following commands: voice class sip-profiles , response , request , voice-class sip copy-list , sip-header

Prerequisites

- Configuring the **media flow-around** command is required for Session Description Protocol (SDP) pass-through. When flow-around is not configured, the flow-through mode of SDP pass-through will be functional.
- When the dial-peer media flow mode is asymmetrically configured, the default behavior is to fall back to SDP pass-through with flow-through.

Restrictions

When Session Description Protocol (SDP) pass-through is enabled, some of the interworking that the CUBE currently performs cannot be activated. These features include:

- Delayed Offer to Early Offer Interworking
- Supplementary Services with Triggered Invites
- Flow-around calls will not work with SDP pass through
- DTMF Interworking Scenarios
- Fax Interworking/QoS Negotiation
- Transcoding

For configurable pass-through of SIP INVITE parameters, the following features for Session Initiation Protocol (SIP)-SIP dial-peer rotary calls are not supported:

- Unsupported header pass-through functionality for SIP-SIP dial-peer rotary calls
- Unsupported content pass-through functionality for SIP-SIP dial-peer rotary calls



Note With CSCty41575, the unsupported header and content pass-through functionalities mentioned above are addressed.

Supported SIP Headers

Mandatory SIP Headers

The following table provides a list of mandatory headers:

Table 45: List of Mandatory Headers

Also	Authorization	Call_ID
CC-Diversion	CC-Redirect	Cisco_Gcid
Cisco_Ccid	Contact	Content-Disposition

Content-Encoding	Content-Length	Content-Type
Cseq	Date	From
Max-Forwards	MIME-Version	P-Asserted-Identity
P-Preferred-Identity	Privacy	Proxy-Authenticate
Proxy-Authorization	Record-Route	Route
Session-Expires	Timestamp	To
User-Agent	Via	WWW-Authenticate

Unsupported Headers

You can configure CUBE to pass through unsupported headers (headers CUBE cannot understand). The following are some of the examples for SIP headers that are unsupported on CUBE:

- P-Early-Media
- SIP-Req-URI

Enable Configurable Pass-Through of SIP INVITE Parameters (Global Level)

Perform this task to configure unsupported content pass-through on a CUBE platform at the global level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **pass-thru {content {sdp | un supp} | headers {un supp | list-tag}}**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Global Level)

	Command or Action	Purpose
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# <code>voice service voip</code>	Enters voice service VoIP configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# <code>sip</code>	Enters SIP configuration mode.
Step 5	pass-thru {content {sdp unsupp} headers {unsupp list-tag}} Example: Device(conf-serv-sip)# <code>pass-thru content unsupp</code>	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.
Step 6	end Example: Device(conf-serv-sip)# <code>end</code>	Ends the current configuration session and returns to privileged EXEC mode.

Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Global Level)

```

Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# pass-thru content unsupp
Device(conf-serv-sip)# end

```

Enable Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level)

Perform this task to configure unsupported content pass-through on a CUBE platform at the dial-peer level.

SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip pass-thru {content {sdp | unsupp} | headers {unsupp | list tag}} [system]**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# dial-peer voice 2 voip	Enters dial peer VoIP configuration mode.
Step 4	voice-class sip pass-thru {content {sdp unsupp} headers {unsupp list tag}} [system] Example: Device(config-dial-peer)# voice-class sip pass-thru content sdp	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.
Step 5	end Example: Device(config-dial-peer)# end	Ends the current configuration session and returns to privileged EXEC mode.

Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level)

```

Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# voice-class sip pass-thru content sdp
Device(config-dial-peer)# end

```

Configure a Route String Header Pass-Through Using Pass-Through List

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-hdr-passthru list-tag**
4. **passthru-hdr header-name**
5. **passthru-hdr-unsupp**
6. **exit**
7. **dial-peer voice tag voip**
8. **description string**
9. **session protocol sipv2**
10. **voice-class sip pass-thru headers list-tag**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class sip-hdr-passthru list-tag Example: Device(config)# voice class sip-hdr-passthru list 101	Configures list of headers to be passed through and enters voice class configuration mode.
Step 4	passthru-hdr header-name Example: Device(config-class)# passthru-hdr Resource-Priority	Adds header name to the list of headers to be passed through. Repeat this step for every non-mandatory header.
Step 5	passthru-hdr-unsupp Example: Device(config-class)# passthru-hdr-unsupp	Adds the unsupported headers to the list of headers to be passed through.

	Command or Action	Purpose
Step 6	exit Example: Device(config-class)# exit	Exits the current configuration session and returns to global configuration mode.
Step 7	dial-peer voice tag voip Example: Device(config)# dial-peer voice 1 voip	Enters dial peer voice configuration mode.
Step 8	description string Example: Device(config-dial-peer)# description inbound-dialpeer	Adds descriptive information about the dial peer.
Step 9	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the IETF Session Initiation Protocol (SIP) for the dial peer.
Step 10	voice-class sip pass-thru headers list-tag Example: Device(config-dial-peer)# voice-class sip pass-thru headers 101	Enables call routing based on the destination route string for a dial peer.
Step 11	end Example: Device(config-dial-peer)# end	Exits the current configuration mode and returns to privileged EXEC mode.

Example: Configuring a Route String Header Pass-Through Using Pass-Through List

```

Device> enable
Device# configure terminal
Device(config)# voice class sip-hdr-passthru list 101
Device(config-class)# passthru-hdr X-hdr-1
Device(config-class)# passthru-hdr Resource-Priority
Device(config-class)# passthru-hdr-unsupp
Device(config-class)# exit
Device(config)# dial-peer voice 1 voip
Device(config-dial-peer)# description inbound-dialpeer
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# voice-class sip pass-thru headers 101
Device(config-dial-peer)# end

```

Example: Passing a Header Not Supported by CUBE

CUBE does not pass “x-cisco-tip”. However, certain TelePresence equipments require “TIP”.

The SIP profile below will look for "x-cisco-tip" in the inbound contact header then pass it in the outbound contact header.

Inbound Contact Header

```
Contact: <sip:89016442998@161.44.77.193;transport=udp>;x-cisco-tip
```

Outbound Contact Header

```
Contact: <sip:89016442998@10.86.176.19:5060>;x-cisco-tip
```

Create a copylist to pass the Contact Header from the incoming message to the outgoing message. The “x-cisco-tip” is not copied in this step as it is unsupported by CUBE.

```
!Create a copyList
Device(config)# voice class sip-copylist 1
Device(config-class)# sip-header Contact
Device(config-class)# exit
```

!Apply the copylist to incoming dial peer.

```
Device(config)# dial-peer voice 1 voip
Device(config-dial-peer)# description incoming SIP Trunk
Device(config-dial-peer)# incoming called-number
Device(config-dial-peer)# voice-class sip copy-list 1
```

Create a SIP profile that copies “x-cisco-tip” into a variable, and use that variable to modify the outgoing Contact header. Apply the SIP profile to an outbound dial peer.

```
Device# voice class sip-profiles 3001
```

!Copy the Contact header from the incoming dial peer into variable u01

```
Device(config-class)# request INVITE peer-header sip Contact copy "(;x-cisco-tip)" u01
```

!Modify the outgoing SIP Invite with this variable.

```
Device(config-class)# request INVITE sip-header Contact modify "$" "\u01"
```

!Apply the SIP Profile to the outgoing dial peer.

```
Device(config)# dial-peer voice 5000 voip
Device(config-dial-peer)# description outbound SIP
Device(config-dial-peer)# destination-pattern 5...$
Device(config-dial-peer)# voice-class sip profiles 3001
```



PART VI

Protocol Interworking

- [Basic SIP Configuration, on page 283](#)
- [Configurable SIP Parameters via DHCP, on page 303](#)
- [Delayed Offer to Early Offer, on page 317](#)
- [SIP: RFC 2782 Compliance with DNS SRV Queries, on page 325](#)
- [Mid-call Signaling, on page 331](#)
- [Early Dialog UPDATE Block , on page 341](#)
- [Forked 18x Responses , on page 347](#)
- [Pass-Through of Unsupported Content Types in SIP INFO Messages, on page 353](#)
- [Support for PAID, PPID, Privacy, PCPID, and PAURI Headers , on page 355](#)
- [Dynamic REFER Handling, on page 377](#)
- [Cause Code Mapping, on page 385](#)



CHAPTER 29

Basic SIP Configuration

- [Overview, on page 283](#)
- [SIP Configuration Fundamentals, on page 284](#)
- [Configuration Examples, on page 297](#)
- [Toll Fraud Prevention, on page 301](#)

Overview

This chapter provides basic configuration information for the following features:

- SIP Register Support
- SIP Redirect Processing
- SIP 300 Multiple Choice Messages
- Interaction with Forking Proxies
- SIP Intra-Gateway Hairpinning



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Finding Support Information for Platforms and Cisco Software Images

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

SIP Register Support

SIP gateways allow registration of E.164 numbers to a SIP proxy or registrar server on behalf of analog phone voice ports (FXS), IP phone virtual voice ports (Ephone-dn Virtual FXS Voice port), and local SCCP phones. By default, SIP gateways do not generate SIP Register messages. The following tasks set up the gateway to register E.164 phone numbers with an external SIP registrar.



Note There are no commands that allow registration with the SIP protocols.

SIP Configuration Fundamentals



Note For help with a procedure, see the verification and troubleshooting sections.

Configure SIP VoIP Services on a CUBE Gateway

Shut Down or Enable VoIP Service on CUBE Gateways

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `[no] shutdown [forced]`
5. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Router(config)# voice service voip	Enters voice-service VoIP configuration mode.
Step 4	[no] shutdown [forced] Example: Router(config-voi-serv)# shutdown forced	Shuts down or enables VoIP call services.

	Command or Action	Purpose
Step 5	exit Example: Router(config-voi-serv)# exit	Exits the current mode.

Shut Down or Enable VoIP Submodes on Cisco Gateways

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. [no] call service stop [forced] [maintain-registration]
6. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Router(config)# voice service voip	Enters voice-service VoIP configuration mode.
Step 4	sip Example: Router(config-voi-serv)# sip	Enters SIP configuration mode.
Step 5	[no] call service stop [forced] [maintain-registration] Example: Router(conf-serv-sip)# call service stop maintain-registration	Shuts down or enables VoIP call services for the selected submode.

	Command or Action	Purpose
Step 6	exit Example: <pre>Router(conf-serv-sip)# exit</pre>	Exits the current mode.

Configure SIP Register Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **registrar {dns: address | ipv4: destination-address} expires seconds [tcp] [secondary]**
5. **retry register number**
6. **timers register milliseconds**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	sip-ua Example: <pre>Router(config)# sip-ua</pre>	Enters SIP user-agent configuration mode.
Step 4	registrar {dns: address ipv4: destination-address} expires seconds [tcp] [secondary] Example: <pre>Router(config-sip-ua)# registrar ipv4:10.8.17.40 expires 3600 secondary</pre>	Registers E.164 numbers on behalf of analog phone voice ports (FXS) and IP phone virtual voice ports (EFXS) with an external SIP proxy or SIP registrar server. Keywords and arguments are as follows: <ul style="list-style-type: none"> • dns: address --Domain-name server that resolves the name of the dial peer to receive calls. • ipv4: destination-address --IP address of the dial peer to receive calls. • expires seconds Default registration time, in seconds.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • tcp --Sets transport layer protocol to TCP. UDP is the default. • secondary --Specifies registration with a secondary SIP proxy or registrar for redundancy purposes. Optional.
Step 5	retry register <i>number</i> Example: <pre>Router(config-sip-ua)# retry register 6</pre>	Use this command to set the total number of SIP Register messages that the gateway should send. The argument is as follows: <ul style="list-style-type: none"> • number --Number of Register message retries. Range: 1–10. Default: 6.
Step 6	timers register <i>milliseconds</i> Example: <pre>Router(config-sip-ua)# timers register 500</pre>	Use this command to set how long the SIP user agent waits before sending register requests. The argument is as follows: <ul style="list-style-type: none"> • milliseconds --Waiting time, in ms. Range: 100–1000. Default: 500.
Step 7	exit Example: <pre>Router(config-sip-ua)# exit</pre>	Exits the current mode.

Configure SIP Redirect Processing

Configure Call-Redirect Processing

Redirect processing using the **redirection** command is enabled by default. To disable and then reset redirect processing, perform the steps listed in this section:

IP-to-IP call redirection can be enabled globally or on a dial-peer basis. To configure, perform the steps listed in these sections:

Configure Call-Redirect Processing Enhancement

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **no redirection**
5. **redirection**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	sip-ua Example: Router(config)# sip-ua	Enters SIP user-agent configuration mode.
Step 4	no redirection Example: Router(config-sip-ua)# no redirection	Disables redirect handling--causes the gateway to treat incoming 3xx responses as 4xx error class responses.
Step 5	redirection Example: Router(config-sip-ua)# redirection	Resets call redirection to work as specified in RFC 2543. The command default redirection also resets call redirection to work as specified in RFC 2543.
Step 6	exit Example: Router(config-sip-ua)# exit	Exits the current mode.

Configure Call Redirect to Support Calls on a Specific VoIP Dial Peer

**Note**

- To specify IP-to-IP call redirection for a specific VoIP dial peer, configure it on an inbound dial peer in dial-peer configuration mode. The default application supports IP-to-IP redirection.
- When IP-to-IP redirection is configured in dial-peer configuration mode, the configuration on the specific inbound dial peer takes precedence over the global configuration that is entered under voice service configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **dial-peer voice** *tag* **voip**
4. **application** *application-name*
5. **redirect ip2ip**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>tag</i> voip Example: Router(config)# dial-peer voice 29 voip	Use this command to enter dial-peer configuration mode. The argument is as follows: <i>tag</i> --Digits that define a particular dial peer. Range: 1 to 2,147,483,647 (enter without commas).
Step 4	application <i>application-name</i> Example: Router(config-dial-peer)# application session	Enables a specific application on a dial peer. The argument is as follows: <i>application-name</i> --Name of the predefined application you wish to enable on the dial peer. For SIP, the default Tcl application (from the Cisco IOS image) is session and can be applied to both VoIP and POTS dial peers. The application must support IP-to-IP redirection.
Step 5	redirect ip2ip Example: Router(conf-dial-peer)# redirect ip2ip	Redirects SIP phone calls to a SIP phone calls on a specific VoIP dial peer using the Cisco IOS voice gateway.
Step 6	exit Example: Router(conf-dial-peer)# exit	Exits the current mode.

Configure SIP Implementation

Minor underlying or minimally configurable features are described in the following sections:

For additional information on SIP implementation enhancements, see “[Achieving SIP RFC Compliance.](#)”

Interaction with Forking Proxies

Call forking enables the terminating gateway to handle multiple requests and the originating gateway to handle multiple provisional responses for the same call. Call forking is required for the deployment of the *find me/follow me* type of services.

Support for call forking enables the terminating gateway to handle multiple requests and the originating gateway to handle multiple provisional responses for the same call. Interaction with forking proxies applies to gateways acting as a UAC, and takes place when a user is registered to several different locations. When the UAC sends an INVITE message to a proxy, the proxy forks the request and sends it to multiple user agents. The SIP gateway processes multiple 18X responses by treating them as independent transactions under the same call ID. When the relevant dial peers are configured for QoS, the gateway maintains state and initiates RSVP reservations for each of these independent transactions. When it receives an acknowledgment, such as a 200 OK, the gateway accepts the successful acknowledgment and destroys state for all other transactions.

The forking feature sets up RSVP for each transaction *only* if the dial peers are configured for QoS. If not, the calls proceed as best-effort.

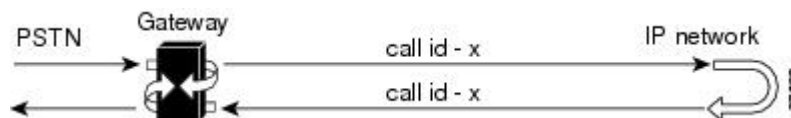
Support for interaction with forking proxies applies only to gateways acting as UACs. It does not apply when the gateway acts as a UAS. In that case, the proxy forks multiple INVITES with the same call ID to the same gateway but with different request URLs.

Also, the forking feature sets up RSVP for each transaction *only* if the dial peers are configured for QoS. If not, the calls proceed as best-effort.

SIP Intra-Gateway Hairpinning

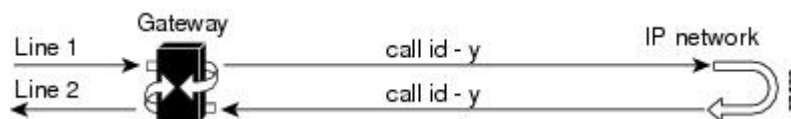
SIP hairpinning is a call routing capability in which an incoming call on a specific gateway is signaled through the IP network and back out the same gateway. This can be a PSTN call routed into the IP network and back out to the PSTN over the same gateway (see the figure below).

Figure 24: PSTN Hairpinning Example



Similarly, SIP hairpinning can be a call signaled from a line (for example, a telephone line) to the IP network and back out to a line on the same access gateway (see the figure below).

Figure 25: Telephone Line Hairpinning Example



With SIP hairpinning, unique gateways for ingress and egress are unnecessary.

SIP supports plain old telephone service (POTS)-to-POTS hairpinning (which means that the call comes in one voice port and is routed out another voice port). It also supports POTS-to-IP call legs and IP-to-POTS call legs. However, it does not support IP-to-IP hairpinning. This means that the SIP gateway cannot take an inbound SIP call and reroute it back to another SIP device using the VoIP dial peers.

Only minimal configuration is required for this feature. To enable hairpinning on the SIP gateway, see the following configuration example for dial peers. Note that:

- The POTS dial peer must have preference 2 defined, and the VoIP dial peer must have preference 1 defined. This ensures that the call is sent out over IP, not Plain Old Telephone Service (POTS).
- The session target is the same gateway because the call is being redirected to it.

```
!  
dial-peer voice 53001 pots  
  preference 2  
  destination-pattern 5300001  
  prefix 5300001  
!  
dial-peer voice 53002 pots  
  preference 2  
  destination-pattern 5300002  
  prefix 5300002  
!  
dial-peer voice 530011 voip  
  preference 1  
  destination-pattern 5300001  
  session protocol sipv2  
  session target ipv4:10.1.1.41  
  playout-delay maximum 300  
  codec g711alaw  
!  
dial-peer voice 530022 voip  
  preference 1  
  destination-pattern 5300002  
  session protocol sipv2  
  session target ipv4:10.1.1.41  
  playout-delay maximum 300  
  codec g711alaw
```

Verify CUBE Status

To verify CUBE status and configuration, perform the following steps as appropriate (commands are listed in alphabetical order).

SUMMARY STEPS

1. **show sip service**
2. **show sip-ua register status**
3. **show sip-ua statistics**
4. **show sip-ua status**
5. **show sip-ua timers**

DETAILED STEPS

Step 1 **show sip service**

Use this command to display the status of SIP call service on a SIP gateway.

The following sample output shows that SIP call service is enabled:

Example:

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

The following sample output shows that SIP call service was shut down with the **shutdown** command:

Example:

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

The following sample output shows that SIP call service was shut down with the **call service stop** command:

Example:

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

The following sample output shows that SIP call service was shut down with the **shutdown forced** command:

Example:

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

The following sample output shows that SIP call service was shut down with the **call service stop forced** command:

Example:

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

Step 2 show sip-ua register status

Use this command to display the status of E.164 numbers that a SIP gateway has registered with an external primary SIP registrar.

Example:

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

Step 3 show sip-ua statistics

Use this command to display response, traffic, and retry SIP statistics, including whether call redirection is disabled.

The following sample shows that four registers were sent:

Example:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Informational:
  Trying 0/0, Ringing 0/0,
```

```

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

```

The following sample output shows the RedirectResponseMappedToClientError status message. An incremented number indicates that 3xx responses are to be treated as 4xx responses. When call redirection is enabled (default), the RedirectResponseMappedToClientError status message is not incremented.

Example:

```

Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Informational:
Trying 0/0, Ringing 0/0,

```

```

    Forwarded 0/0, Queued 0/0,
    SessionProgress 0/0
Success:
    OkInvite 0/0, OkBye 0/0,
    OkCancel 0/0, OkOptions 0/0,
    OkPrack 0/0, OkPreconditionMet 0/0,
    OKSubscribe 0/0, OkNotify 0/0,
    202Accepted 0/0
Redirection (Inbound only):
    MultipleChoice 0, MovedPermanently 0,
    MovedTemporarily 0, UseProxy 0,
    AlternateService 0
Client Error:
    BadRequest 0/0, Unauthorized 0/0,
    PaymentRequired 0/0, Forbidden 0/0,
    NotFound 0/0, MethodNotAllowed 0/0,
    NotAcceptable 0/0, ProxyAuthReqd 0/0,
    ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
    ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
    UnsupportedMediaType 0/0, BadExtension 0/0,
    TempNotAvailable 0/0, CallLegNonExistent 0/0,
    LoopDetected 0/0, TooManyHops 0/0,
    AddrIncomplete 0/0, Ambiguous 0/0,
    BusyHere 0/0, RequestCancel 0/0
    NotAcceptableMedia 0/0, BadEvent 0/0
Server Error:
    InternalError 0/0, NotImplemented 0/0,
    BadGateway 0/0, ServiceUnavail 0/0,
    GatewayTimeout 0/0, BadSipVer 0/0,
    PreCondFailure 0/0
Global Failure:
    BusyEverywhere 0/0, Decline 0/0,
    NotExistAnywhere 0/0, NotAcceptable 0/0
Miscellaneous counters:
    RedirectResponseMappedToClientError 1,
SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 0/0, Ack 0/0, Bye 0/0,
    Cancel 0/0, Options 0/0,
    Prack 0/0, Comet 0/0,
    Subscribe 0/0, Notify 0/0,
    Refer 0/0
Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0,
    Prack 0, Comet 0, Reliable1xx 0, Notify 0
SDP application statistics:
    Parses: 0, Builds 0
    Invalid token order: 0, Invalid param: 0
    Not SDP desc: 0, No resource: 0

```

Step 4 show sip-ua status

Use this command to display status for the SIP user agent (UA), including whether call redirection is enabled or disabled.

Example:

```

Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 1 (rfc 2052)
Redirection (3xx) message handling: ENABLED

```


Step 5 **show sip-ua timers**

Use this command to display the current settings for the SIP user-agent (UA) timers.

The following sample output shows the waiting time before a register request is sent--that is, the value that is set with the **timers register** command:

Example:

```
Router# show sip-ua timers
SIP UA Timer Values (milliseconds)
trying 500, expires 180000, connect 500, disconnect 500
comet 500, prack 500, rellxx 500, notify 500
refer 500, register 500
```

Tips to Troubleshoot

For more information on troubleshooting, see the following references:

- "Cisco IOS Voice Troubleshooting and Monitoring Guide"
- Cisco Technical Support at <http://www.cisco.com/en/US/support/index.html>
- *Cisco IOS Debug Command Reference*
- *Cisco IOS Voice, Video, and Fax Configuration Guide*
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [VoIP Debug Commands](#)



Note Commands are listed in alphabetical order.

- Verify that SIP-supported codecs are used. Support for codecs varies on different platforms; use the **codec ?** command to determine the codecs available on a specific platform.
- Use the **debug aaa authentication** command to display high-level diagnostics that are related to AAA logins.
- Use the **debug asnl events** command to verify that the SIP subscription server is up. The output displays a pending message if, for example, the client is unsuccessful in communicating with the server.
- Use the **debug ccsip** family of commands for general SIP debugging, including viewing direction-attribute settings and port and network address-translation traces. Use any of the following related commands:
 - **debug ccsip all**--Enables all SIP-related debugging
 - **debug ccsip calls**--Enables tracing of all SIP service-provider interface (SPI) calls
 - **debug ccsip error**--Enables tracing of SIP SPI errors.
 - **debug ccsip events**--Enables tracing of all SIP SPI events

- **debug ccsip info**--Enables tracing of general SIP SPI information, including verification that call redirection is disabled
 - **debug ccsip media**--Enables tracing of SIP media streams
 - **debug ccsip messages**--Enables all SIP SPI message tracing, such as those that are exchanged between the SIP user-agent client (UAC) and the access server
 - **debug ccsip preauth**--Enables diagnostic reporting of authentication, authorization, and accounting (AAA) preauthentication for SIP calls
 - **debug ccsip states**--Enables tracing of all SIP SPI state tracing
 - **debug ccsip transport**--Enables tracing of the SIP transport handler and the TCP or User Datagram Protocol (UDP) process
- Use the **debug isdn q931** command to display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network.
 - Use the **debug kpml** command to enable debug tracing of KeyPad Markup Language (KPML) parser and builder errors.
 - Use the **debug radius** command to enable debug tracing of RADIUS attributes.
 - Use the **debug rpms-proc preauth** command to enable debug tracing on the Cisco RPMS process for SIP calls.
 - Use the **debug rtr trace** command to trace the execution of an SAA operation.
 - Use the **debug voip** family of commands, including the following:
 - **debug voip ccapi protoheaders** --Displays messages sent between the originating and terminating gateways. If no headers are being received by the terminating gateway, verify that the **header-passing** command is enabled on the originating gateway.
 - **debug voip ivr script**--Displays any errors that might occur when the Tcl script is running.
 - **debug voip rtp session named-event 101** --Displays information important to DTMF-relay debugging, if you are using codec types g726r16 or g726r24. Be sure to append the argument *101* to the command to prevent the console screen from flooding with messages and all calls from failing.

Sample output for some of these commands follows:

Sample Output for the debug ccsip events Command

- The example shows how the Proxy-Authorization header is broken down into a decoded username and password.

```
Router# debug ccsip events
CCSIP SPI: SIP Call Events tracing is enabled
21:03:21: sippmh_parse_proxy_auth: Challenge is 'Basic'.
21:03:21: sippmh_parse_proxy_auth: Base64 user-pass string is 'MTIzNDU2Nzg5MDEyMzQ1NjJou'.
21:03:21: sip_process_proxy_auth: Decoded user-pass string is '1234567890123456:.'.
21:03:21: sip_process_proxy_auth: Username is '1234567890123456'.
21:03:21: sip_process_proxy_auth: Pass is '.'.
21:03:21: sipSPIAddBillingInfoToCcb: sipCallId for billing records =
10872472-173611CC-81E9C73D-F836C2B6@172.18.192.19421:03:21: ****Adding to UAS Request table
```

Sample Output for the debug ccsip info Command

This example shows only the portion of the debug output that shows that call redirection is disabled. When call redirection is enabled (default), there are no debug line changes.

```
Router# debug ccsip info
00:20:32: HandleUdpSocketReads :Msg enqueued for SPI with IPAddr: 172.18.207.10
:5060
00:20:32: CCSIP-SPI-CONTROL: act_sentinvite_new_message
00:20:32: CCSIP-SPI-CONTROL: sipSPICheckResponse
00:20:32: sip_stats_status_code
00:20:32: ccsip_get_code_class: !!Call Redirection feature is disabled on the GW
00:20:32: ccsip_map_call_redirect_responses: !!Mapping 302 response to 480
00:20:32: Roundtrip delay 4 milliseconds for method INVITE
```

Configuration Examples

SIP Register Support Example

```
Current configuration : 3394 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
memory-size iomem 15
ip subnet-zero
!
no ip domain lookup
!
voice service voip
  redirect ip2ip
sip
  redirect contact order best-match
ip dhcp pool vespa
  network 192.168.0.0 255.255.255.0
  option 150 ip 192.168.0.1
  default-router 192.168.0.1
!
voice call carrier capacity active
!
voice class codec 1
  codec preference 2 g711ulaw
!
no voice hpi capture buffer
no voice hpi capture destination
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Ethernet0/0
  ip address 10.8.17.22 255.255.0.0
  half-duplex
!
interface FastEthernet0/0
  ip address 192.168.0.1 255.255.255.0
```

```

speed auto
no cdp enable
h323-gateway voip interface
h323-gateway voip id vespa2 ipaddr 10.8.15.4 1718
!
router rip
network 10.0.0.0
network 192.168.0.0
!
ip default-gateway 10.8.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.8.0.1
no ip http server
ip pim bidir-enable
!
tftp-server flash:SEPDEFAULT.cnf
tftp-server flash:P005B302.bin
call fallback active
!
call application global default.new
call rsvp-sync
!
voice-port 1/0
!
voice-port 1/1
!
mgcp profile default
!
dial-peer voice 1 pots
destination-pattern 5100
port 1/0
!
dial-peer voice 2 pots
destination-pattern 9998
port 1/1
!
dial-peer voice 123 voip
destination-pattern [12]...
session protocol sipv2
session target ipv4:10.8.17.42
dtmf-relay sip-notify
!
gateway
!
sip-ua
retry invite 3
retry register 3
timers register 150
registrar dns:myhost3.example.com expires 3600
registrar ipv4:10.8.17.40 expires 3600 secondary
!
telephony-service
max-dn 10
max-conferences 4
!
ephone-dn 1
number 4001
!
ephone-dn 2
number 4002
!
line con 0
exec-timeout 0 0
line aux 0

```

```
line vty 0 4
login
line vty 5 15
login
!
no scheduler allocate
end
```

SIP 300 Multiple Choice Messages Example

This section provides a configuration example showing redirect contact order set to best match.

```
Current configuration : 3394 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
memory-size iomem 15
ip subnet-zero
!
no ip domain lookup
!
voice service voip
redirect ip2ip
sip
redirect contact order best-match
ip dhcp pool vespa
network 192.168.0.0 255.255.255.0
option 150 ip 192.168.0.1
default-router 192.168.0.1
!
voice call carrier capacity active
!
voice class codec 1
codec preference 2 g711ulaw
!
no voice hpi capture buffer
no voice hpi capture destination
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Ethernet0/0
ip address 10.8.17.22 255.255.0.0
half-duplex
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
speed auto
no cdp enable
h323-gateway voip interface
h323-gateway voip id vespa2 ipaddr 10.8.15.4 1718
!
router rip
network 10.0.0.0
network 192.168.0.0
!
ip default-gateway 10.8.0.1
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.8.0.1
no ip http server
ip pim bidir-enable
!
tftp-server flash:SEPDEFAULT.cnf
tftp-server flash:P005B302.bin
call fallback active
!
call application global default.new
call rsvp-sync
!
voice-port 1/0
!
voice-port 1/1
!
mgcp profile default
!
dial-peer voice 1 pots
 destination-pattern 5100
 port 1/0
!
dial-peer voice 2 pots
 destination-pattern 9998
 port 1/1
!
dial-peer voice 123 voip
 destination-pattern [12]...
 session protocol sipv2
 session target ipv4:10.8.17.42
 dtmf-relay sip-notify
!
gateway
!
sip-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar dns:myhost3.example.com expires 3600
 registrar ipv4:10.8.17.40 expires 3600 secondary
!
telephony-service
 max-dn 10
 max-conferences 4
!
ephone-dn 1
 number 4001
!
ephone-dn 2
 number 4002
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
line vty 5 15
 login
!
no scheduler allocate
end
```

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS Software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Cisco Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (CUBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- **Disable secondary dial tone on voice ports**--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for Foreign Exchange Office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- **Cisco router access control lists (ACLs)**--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized SIP calls from unknown parties to be processed and connected by the router or gateway.
- **Close unused SIP ports**--If either the SIP protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers that are configured to route calls outbound to the PSTN using either time division multiplexing (TDM) trunks or IP, close the unused SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- **Change SIP port 5060**--If SIP is actively used, consider changing the port to something other than well-known port 5060.
- **SIP registration**--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- **SIP Digest Authentication**--If the SIP Digest Authentication feature is available for either registrations or invites, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- **Explicit incoming and outgoing dial peers**--Use explicit dial peers to control the types and parameters of calls that are allowed by the router, especially in IP-to-IP connections on Cisco Unified CME, SRST, and CUBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- **Explicit destination patterns**--Use dial peers with more granularity than T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- **Translation rules**--Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- **Tcl and VoiceXML scripts**--Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus

DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.

- Host name validation--Use the “permit hostname” feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DDNS)--If you are using DDNS as the “session target” on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DDNS responses (which are used later for call setup destinations).

For more configuration guidance, see the “[Cisco IOS Unified Communications Manager Express Toll Fraud Prevention](#)” paper.



CHAPTER 30

Configurable SIP Parameters via DHCP

- [Overview, on page 303](#)
- [Prerequisites, on page 307](#)
- [Restrictions for Configurable SIP Parameters via DHCP, on page 307](#)
- [Configure SIP Parameters via DHCP, on page 308](#)

Overview

The Configurable SIP Parameters via DHCP feature allows a Dynamic Host Configuration Protocol (DHCP) server to provide Session Initiation Protocol (SIP) parameters via a DHCP client. These parameters are used for user registration and call routing.

The DHCP server returns the SIP Parameters via DHCP options 120 and 125. These options are used to specify the SIP user registration and call routing information. The SIP parameters returned are the SIP server address via Option 120, and vendor-specific information such as the pilot, contract or primary number, an additional range of secondary numbers, and the SIP domain name via Option 125.

In the event of changes to the SIP parameter values, this feature also allows a DHCP message called DHCPFORCERENEW to reset or apply a new set of values.

The SIP parameters provisioned by DHCP are stored, so that on reboot they can be reused.

To perform basic Configurable SIP Parameters via DHCP configuration tasks, you should understand the following concepts:

Cisco Unified Border Element (CUBE) Support for Configurable SIP Parameters via DHCP

The CUBE provides the support for the DHCP provisioning of the SIP parameters.

The NGN is modeled using SIP as a VoIP protocol. In order to connect to NGN, the User to Network Interface (UNI) specification is used. Cisco TelePresence Systems (CTS), consisting of an IP Phone, a codec, and Cisco Unified Communications Manager, are required to interconnect over the NGN for point-to-point and point-to-multipoint video calls. Because Cisco Unified Communications Manager does not provide a UNI interface, there has to be an entity to provide the UNI interface. The CUBE provides the UNI interface and has several advantages such as demarcation, delayed offer to early offer, and registration.

The figure below shows the CUBE providing the UNI interface for the NGN.

Figure 26: Cisco NGN with CCUBE providing UNI interface



DHCP to Provision SIP Server, Domain Name, and Phone Number

NGN requires CUBE to support DHCP (RFC 2131 and RFC 2132) to provision the following:

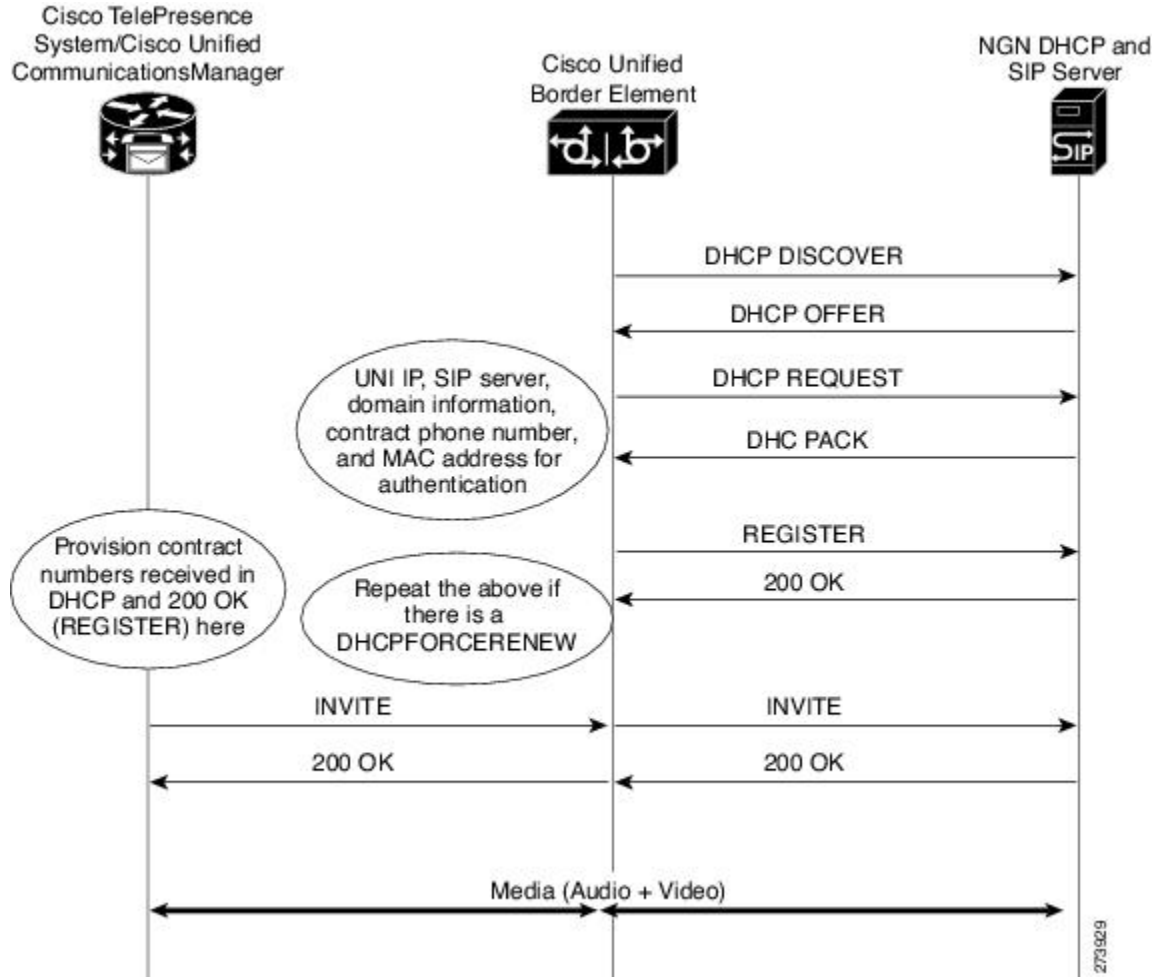
- IP address for CUBE's UNI interface facing NGN
- SIP server address using option 120
- Option 125 vendor specific information to get:
 - Pilot number (also called primary or contract number), there is only one pilot number in DHCPACK, and REGISTER is done only for the pilot number
 - Additional numbers, or secondary numbers, are in DHCPACK; there is no REGISTER for additional numbers
 - SIP domain name
- DHCPFORCERENEW to reset or apply a new set of SIP parameters (RFC 3203)

DHCP-SIP Call Flow

The following scenario shows the DHCP messages involved in provisioning information such as the IP address for UNI interface, and SIP parameters including the SIP server address, phone number, and domain name, along with how SIP messages use the provisioned information.

The figure below shows the DHCP and SIP messages involved in obtaining the SIP parameters and using them for REGISTER and INVITE.

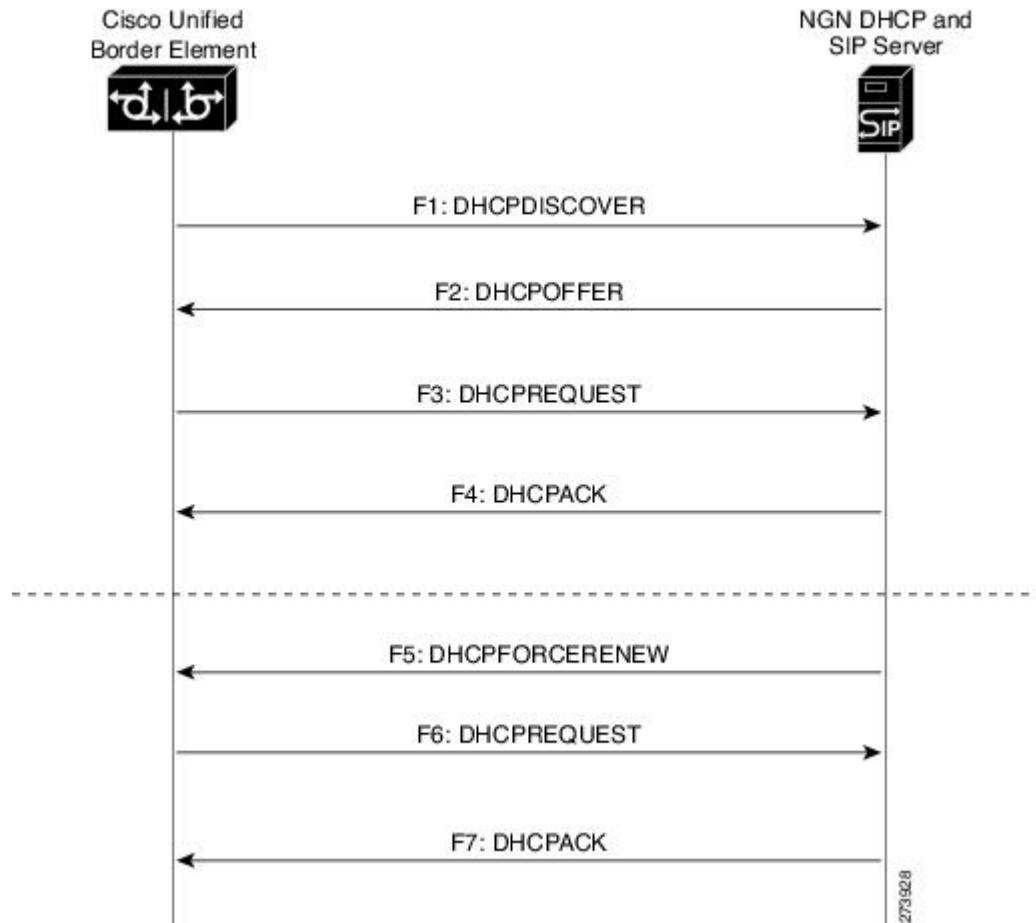
Figure 27: DHCP-SIP Call Flow



DHCP Message Details

The DHCP call flow involved in obtaining CUBE provision information, including the IP address for UNI interface and SIP information such as phone number, domain, and SIP server, is shown in the figure below.

Figure 28: DHCP Message Details



The DHCP messages involved in provisioning the SIP parameters are described in Steps 1 to 6.

1. F1: The CUBE DHCP client sends a DHCPDISCOVER message to find the available NGN DHCP servers on the network and obtain a valid IPv4 address. The Cisco Unified Border Element DHCP client identity (computer name) and MAC address are included in this message.
2. F2: The CUBE DHCP client receives a DHCPOFFER message from each available NGN DHCP server. The DHCPOFFER message includes the offered DHCP server's IPv4 address, the DHCP client's MAC address, and other configuration parameters.
3. F3: The CUBE DHCP client selects an NGN DHCP server and its IPv4 address configuration from the DHCPOFFER messages it receives, and sends a DHCPREQUEST message requesting its usage. Note that this is where CUBE requests SIP server information via DHCP Option 120 and vendor-identifying information via DHCP Option 125.
4. F4: The chosen NGN DHCP server assigns its IPv4 address configuration to the CUBEDHCP client by sending a DHCPACK message to it. The Cisco Unified Border Element DHCP client receives the DHCPACK message. This is where the SIP server address, phone number and domain name information are received via DHCP options 120 and 125. The CUBE will use the information for registering the phone number and routing INVITE messages to the given SIP server.

5. F5: When NGN has a change of information or additional information (such as changing SIP server address from 1.1.1.1 to 2.2.2.2) for assigning to CUBE, the DHCP server initiates DHCPFORCERENEW to the CUBE. If the authentication is successful, the CUBE DHCP client accepts the DHCPFORCERENEW and moves to the next stage of sending DHCPREQUEST. Otherwise DHCPFORCERENEW is ignored and the current information is retained and used.
6. F6 and F7: In response to DHCPFORCERENEW, similar to steps F3 and F4, the CUBE requests DHCP Options 120 and 125. Upon getting the response, SIP will apply these parameters if they are different by sending an UN-REGISTER message for the previous phone number and a REGISTER message for the new number. Similarly, a new domain and SIP server address will be used. If the returned information is the same as the current set, it is ignored and hence registration and call routing remains the same.

Feature Information

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 46: Feature Information for Configurable SIP Parameters via DHCP

Feature Name	Releases	Feature Information
Configurable SIP Parameters via DHCP	Baseline Functionality	The feature introduces the configuring of SIP parameters via DHCP.

Prerequisites

- A DHCP interface has to be associated with SIP before configurable SIP parameters via DHCP can be enabled.

Restrictions for Configurable SIP Parameters via DHCP

- DHCP Option 120 is the standard DHCP option (RFC3361) to get a SIP server address, and this can be used by any vendor DHCP server. Only one address is supported, which is in the IPv4 address format. Multiple IPv4 address entries are not supported. Also, there is no support for a DNS name in this or for any port number given behind the IPv4 address.
- DHCP Option 125 (RFC 3925) provides vendor-specific information and its interpretation is associated with the enterprise identity. The primary and secondary phone numbers and domain are obtained using Option 125, which is vendor-specific. As long as other customers use the same format as in the Next Generation Network (NGN) DHCP specification, they can use this feature.
- A primary or contract number is required in suboption 202 of DHCP Option 125. There can be only one instance of the primary number and not multiple instances.

- Multiple secondary or numbers in suboption 203 of DHCP Option 125 are supported. Up to five numbers are accepted and the rest ignored. Also, they have to follow the contract number in the DHCP packet data.
- Authentication is not supported for REGISTER and INVITE messages sent from a Cisco Unified Border Element that uses DHCP provisioning
- The DHCP provisioning of SIP Parameters is supported only over one DHCP interface.
- The DHCP option is available only to be configured for the primary registrar. It will not be available for a secondary registrar.

Configure SIP Parameters via DHCP

Configure the DHCP Client

To receive the SIP configuration parameters the CUBE has to act as a DHCP client. This is because in the NGN network, a DHCP server pushes the configuration to a DHCP client. Thus the Cisco Unified Border Element must be configured as a DHCP client.

Perform this task to configure the DHCP client.

Before you begin

You must configure the **ip dhcp client** commands before entering the **ip address dhcp** command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The **ip dhcp client** commands are checked only when an IP address is acquired from DHCP. If any of the **ip dhcp client** commands are entered after an IP address has been acquired from DHCP, the DHCPDISCOVER messages' correct options will not be present or take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip dhcp client request sip-server-address**
5. **ip dhcp client request vendor-identifying-specific**
6. **ip address dhcp**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Router(config)# interface gigabitethernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip dhcp client request sip-server-address Example: Router(config-if)# ip dhcp client request sip-server-address	Configures the DHCP client to request a SIP server address from a DHCP server.
Step 5	ip dhcp client request vendor-identifying-specific Example: Router(config-if)# ip dhcp client request vendor-identifying-specific	Configures the DHCP client to request vendor-specific information from a DHCP server.
Step 6	ip address dhcp Example: Router(config-if)# ip address dhcp	Acquires an IP address on the interface from the DHCP.
Step 7	exit Example: Router(config-if)# exit	Exits the current mode.

Example: Configure the DHCP Client

The following is an example is to enable the DHCP client:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip dhcp client request sip-server-address
Router(config-if)# ip dhcp client request vendor-identifying-specific
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

Enable the SIP Configuration

Enabling the SIP configuration allows the Cisco Unified Border Element to use the SIP parameters received via DHCP for user registration and call routing. Perform this task to enable the SIP configuration.

Before you begin

The **dhcp interface** command has to be entered to declare the interface before the **registrar** and **credential** commands are entered.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **sip-ua**
5. **dhcp interface type number**
6. **registrar dhcp expires seconds random-contact refresh-ratio seconds**
7. **credentials dhcp password [0|7] password realm domain-name**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface type number Example: <pre>Router(config)# interface gigabitethernet 0/0</pre>	Configures an interface type and enters interface configuration mode.
Step 4	sip-ua Example: <pre>Router(config-if)# sip-ua</pre>	Enters SIP user-agent configuration mode.
Step 5	dhcp interface type number Example:	Assigns a specific interface for DHCP provisioning of SIP parameters.

	Command or Action	Purpose
	Router(sip-ua)# dhcp interface gigabitethernet 0/0	<ul style="list-style-type: none"> Multiple interfaces on the CUBE can be configured with DHCP--this command specifies the DHCP interface used with SIP.
Step 6	registrar dhcp expires seconds random-contact refresh-ratio seconds Example: Router(sip-ua)# registrar dhcp expires 100 random-contact refresh-ratio 90	Registers E.164 numbers on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) with an external SIP proxy or SIP registrar server. <ul style="list-style-type: none"> expires seconds --Specifies the default registration time, in seconds. Range is 60 to 65535. Default is 3600. refresh-ratio seconds --Specifies the refresh-ratio, in seconds. Range is 1 to 100 seconds. Default is 80.
Step 7	credentials dhcp password [0 7] password realm domain-name Example: Router(sip-ua)# credentials dhcp password cisco realm cisco.com	Sends a SIP registration message from a Cisco Unified Border Element in the UP state.
Step 8	exit Example: Router(sip-ua)# exit	Exits the current mode.

Enable the SIP Configuration Example

The following is an example to enable the SIP configuration:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/0
Router(config-if)# sip-ua
Router(sip-ua)# dhcp interface gigabitethernet 1/0
Router(sip-ua)# registrar dhcp expires 90 random-contact refresh-ratio 90
Router(sip-ua)# credentials dhcp password cisco realm cisco.com
Router(sip-ua)# exit
```

Tips to Troubleshoot

To display information on DHCP and SIP interaction when SIP parameters are provisioned by DHCP, use the **debug ccsip dhcp** command in privileged EXEC mode.

Configure a SIP Outbound Proxy Server

An outbound-proxy configuration sets the Layer 3 address (IP address) for any outbound REGISTER and INVITE SIP messages. The SIP server can be configured as an outbound proxy server in voice service SIP configuration mode or dial peer configuration mode. When enabled in voice service SIP configuration mode, all the REGISTER and INVITE messages are forwarded to the configured outbound proxy server. When enabled in dial-peer configuration mode, only the messages hitting the defined dial-peer will be forwarded to the configured outbound proxy server.

The configuration tasks in each mode are presented in the following sections:

Perform either of these tasks to configure the SIP server as a SIP outbound proxy server.

Configure a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode

Perform this task to configure the SIP server as a SIP outbound proxy server in voice service SIP configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **outbound-proxy dhcp**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Router(config)# voice service voip	Enters voice service VoIP configuration mode and specifies VoIP as the voice-encapsulation type.
Step 4	sip Example:	Enters voice service SIP configuration mode.

	Command or Action	Purpose
	Router(config-voi-srv)# sip	
Step 5	outbound-proxy dhcp Example: Router(config-serv-sip)# outbound-proxy dhcp	Configures the DHCP client to request a SIP server address from a DHCP server.
Step 6	exit Example: Router(config-serv-sip)# exit	Exits the current mode.

Configure a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode Example

The following is an example to configure a SIP outbound proxy in voice service SIP configuration mode:

```
Router> enable
Router# configure terminal

Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(config-serv-sip)# outbound-proxy dhcp
Router(config-serv-if)# exit
```

Configure a SIP Outbound Proxy Server and Session Target in Dial Peer Configuration Mode

Perform this task to configure the SIP server as a SIP outbound proxy server in dial peer configuration mode.



Note SIP must be configured on the dial peer before DHCP is configured. Therefore the **session protocol sipv2** command must be executed before the **session target dhcp** command. DHCP is supported only with SIP configured on the dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice number voip**
4. **session protocol sipv2**
5. **voice-class sip outbound-proxy dhcp**
6. **session target dhcp**
7. **exit**

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	dial-peer voice number voip Example: Router(config)# dial-peer voice 10 voip	Defines a dial peer, specifies VoIP as the method of voice encapsulation, and enters dial peer configuration mode.
Step 4	session protocol sipv2 Example: Router(config-dial-peer)# session protocol sipv2	Enters the session protocol type as SIP.
Step 5	voice-class sip outbound-proxy dhcp Example: Router(config-dial-peer)# voice-class sip outbound-proxy dhcp	Configures the SIP server received from the DHCP server as a SIP outbound proxy server.
Step 6	session target dhcp Example: Router(config-dial-peer)# session target dhcp	Specifies that the DHCP protocol is used to determine the IP address of the session target.
Step 7	exit Example: Router(config-dial-peer)# exit	Exits the current mode.

Configure a SIP Outbound Proxy Server in Dial Peer Configuration Mode Example

The following is an example of how to configure a SIP outbound proxy in dial peer configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 11 voip
Router(config-dial-peer)# session protocol sipv2
```

```
Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
Router(config-dial-peer)# session target dhcp
Router(config-dial-peer)# exit
```




CHAPTER 31

Delayed Offer to Early Offer

- [Delayed-Offer to Early-Offer, on page 317](#)
- [Delayed-Offer to Early-Offer in Media Flow-Around Calls, on page 317](#)
- [MidCall Renegotiation Support for Delayed-Offer to Early-Offer Calls, on page 322](#)

Delayed-Offer to Early-Offer

The Delayed-Offer to Early-Offer (DO-EO) feature allows CUBE to convert a delayed offer that it receives into an early offer.

This feature also supports midcall renegotiation of codecs required if an exchange of parameters that is not end-to-end causes an inefficient media flow.

Feature Information

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 47: Feature Information for Delayed-Offer to Early-Offer

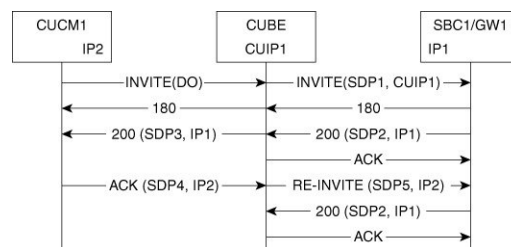
Feature Name	Releases	Feature Information
Delayed-Offer to Early-Offer	Baseline Functionality	The Delayed-Offer to Early-Offer feature allows CUBE to convert a delayed offer it receives into an early offer.

Delayed-Offer to Early-Offer in Media Flow-Around Calls

Delayed-Offer to Early-Offer (DO-EO) allows CUBE to convert a delayed offer (DO) into an early offer (EO) in the media flow-around mode.

CUBE sends its local IP address in the initial EO INVITE Session Description Protocol (SDP) message. In the image, this is illustrated by INVITE (SDP1, CUIP1). Later, an additional RE-INVITE is locally generated by CUBE to communicate the SDP message details from the sender. This is illustrated by RE-INVITE (SDP5, IP2) in the below image. The RE-INVITE response is consumed by CUBE and not communicated to the sender.

Figure 29: Delayed Offer to Early Offer in Media Flow-Around Calls



CUBE supports delayed offer to early offer for SIP-to-SIP video calls. CUBE generates an outgoing Early Offer INVITE with the configured codec list, for an incoming Delayed Offer INVITE.

DO-EO video call is supported if both audio and video codecs are configured under a dial peer. **codec profile** command defines the codec attributes for Video (H263, H264) and Audio (AACLD) codecs. The codec attributes configured under codec-profile is used to generate the a=fmtp attribute line in the Early Offer SDP.

Prerequisites for Delayed-Offer to Early-Offer

Configure delayed-offer to early-offer in media flow-around mode.

Restrictions

- CUBE does not support change in IP address or port number in the locally triggered RE-INVITE response.
- CUBE does not support DO-EO Media Flow-Around for video calls.

Configure Delayed Offer to Early Offer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure conversion of a delayed offer to an early offer:
 - In dial-peer configuration mode
 - voice-class sip early-offer forced**
 - In global VoIP SIP configuration mode
 - early-offer forced**
4. **end**

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	Configure conversion of a delayed offer to an early offer: <ul style="list-style-type: none"> • In dial-peer configuration mode voice-class sip early-offer forced • In global VoIP SIP configuration mode early-offer forced Example: In dial-peer configuration mode: Device (config) dial-peer voice 10 voip Device (config-dial-peer) voice-class sip early-offer forced Device (config-dial-peer) end Example: In global VoIP SIP mode: Device (config)# voice service voip Device (config-voi-serv) sip Device (config-voi-sip) early-offer forced Device (config-voi-sip) end	
Step 4	end	Exits to privileged EXEC mode.

Configure Delayed Offer to Early Offer for Video Calls

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **codec profile** *tag profile*
4. **dial-peer voice number** *number voip*
5. **codec** *codec profile*

6. **video codec** *codec profile*
7. **voice-class sip early-offer forced**
8. **end**

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	codec profile tag profile Example: codec profile 1 aacl codec profile 2 H264	Configures the audio and video codec profiles.
Step 4	dial-peer voice number number voip Example: Device(config)# dial-peer voice 1 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 5	codec codec profile Example: Device(config-dial-peer)# profile 1 aacl	Audio codec profile is applied on the dial peer.
Step 6	video codec codec profile Example: Device(config-dial-peer)# video codec h264 profile 2	Video codec profile is applied on the dial peer.
Step 7	voice-class sip early-offer forced Example: Device (config-dial-peer)# voice-class sip early-offer forced	
Step 8	end	Exits to privileged EXEC mode.

Configure Delayed Offer to Early Offer Media Flow-Around

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media flow-around**
4. Configure conversion of a delayed offer to an early offer:
 - In dial-peer configuration mode
 - voice-class sip early-offer forced**
 - In global VoIP SIP configuration mode
 - early-offer forced**
5. **end**

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	media flow-around Example: Device(config-voi-serv)# media flow-around	Enables media flow-around.
Step 4	Configure conversion of a delayed offer to an early offer: <ul style="list-style-type: none"> • In dial-peer configuration mode <ul style="list-style-type: none"> voice-class sip early-offer forced • In global VoIP SIP configuration mode <ul style="list-style-type: none"> early-offer forced Example: In dial-peer configuration mode: Device (config) dial-peer voice 10 voip Device (config-dial-peer) voice-class sip early-offer forced Device (config-dial-peer) end	

	Command or Action	Purpose
	<p>Example:</p> <p>In global VoIP SIP mode:</p> <pre>Device(config)# voice service voip Device (config-voi-serv) sip Device (config-voi-sip) early-offer forced Device (config-voi-sip) end</pre>	
Step 5	end	Exits to privileged EXEC mode.

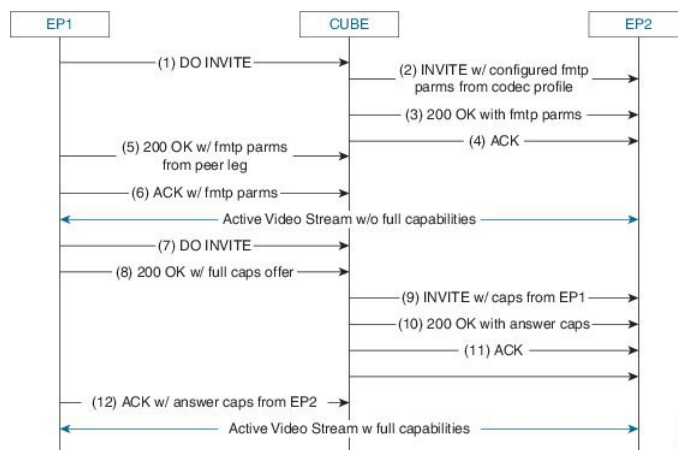
MidCall Renegotiation Support for Delayed-Offer to Early-Offer Calls

When CUBE converts a delayed offer into an early offer, an incomplete exchange of Format specific parameters (FMTP) occurs during call establishment, resulting in either the noninitiation of media transmission or media transmission in a quality that may not be the best. This is especially a problem in video calls.

To overcome this situation, midcall renegotiation of capabilities can be configured.

The **early-offer forced renegotiate [always]** command is used to configure this in global VoIP configuration mode (config-voi-serv) and the **voice-class sip early-offer forced renegotiate** command is dial-peer configuration mode (config-dial-peer) and voice-class configuration mode (config-class).

Figure 30: MidCall Renegotiation of Capabilities



The **early-offer forced renegotiate** command triggers a delayed-offer RE-INVITE if the negotiated codecs are one of the following:

- aacld—Audio codec AACLD 90000 bps
- h263—Video codec H263
- h263+—Video codec H263+
- h264—Video codec H264

- mp4a—Wideband audio codec

The **early-offer forced renegotiate always** command always triggers a delayed-offer RE-INVITE. This option can be used to support all other codecs.

Restrictions for MidCall Renegotiation Support for DO-EO Calls

- If **midcall-signaling block** or **midcall-signaling passthru media-change** commands have been configured, the feature does not work because a midcall RE-INVITE is not triggered by CUBE.
- if initial call is transcoded , then midcall re-invite is not triggered by CUBE.



Note For EO to EO calls, the Delayed-Offer midcall RE-INVITE is not triggered by the CUBE, if either **midcall-signaling block** or **midcall-signaling passthru media-change** command is configured.

Configure Mid Call Renegotiation Support for Delayed-Offer to Early-Offer Calls

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *id* voip**
4. **end**

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	dial-peer voice <i>id</i> voip	Enters dial-peer configuration mode and configures the selected dial peer.
Step 4	end	Exits to privileged EXEC mode.



CHAPTER 32

SIP: RFC 2782 Compliance with DNS SRV Queries

- [Overview, on page 325](#)
- [SIP RFC 2782 Compliance with DNS SRV Queries, on page 326](#)
- [Configure DNS Server Lookups , on page 327](#)
- [Verifying, on page 328](#)

Overview

Effective with Cisco IOS XE Release 2.5, the Domain Name System Server (DNS SRV) query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore "_" character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style.

Feature Information

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 48: Feature Information for SIP: RFC 2782 Compliance with DNS SRV Queries

Feature Name	Releases	Feature Information
SIP: RFC 2782 Compliance of DNS SRV Queries	Cisco IOS XE Release 2.5	Effective with Cisco IOS XE Release 2.5, the DNS SRV query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore "_" character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style. The following command was introduced or modified: srv version .

SIP RFC 2782 Compliance with DNS SRV Queries

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses the DNS SRV query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style originated in RFC 2052. Beginning with Cisco IOS XE Release 2.5, a second style, in compliance with RFC 2782, prepends the protocol label with an underscore "_"; for example, "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style.



Note The DNS SRV lookup is always attempted first for a Fully Qualified Domain Name (FQDN). If the DNS SRV lookup fails CUBE falls back to A-AAAA lookup. If you manually add a port number to a FQDN, the CUBE performs an A-AAAA lookup instead of SRV lookup.

Example:

'session target dns:cisco.com' would perform an SRV lookup and 'session target dns:cisco.com:5060' would perform an A-AAAA lookup.

Configure DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries

Compliance with RFC 2782 changes the DNS SVR protocol label style. RFC 2782 updates RFC 2052 by prepending the protocol label with an underscore character. The prefix format compliant with RFC 2782 is the default format. However, backward compatibility is available, allowing newer versions of Cisco IOS software to work with older networks that support only RFC 2052 DNS SVR prefix style.

To configure the format of DNS SRV queries to comply with RFC 2782, complete this task.



Note You do not have to perform this task if you want to use the default RFC 2782 format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **sip-ua**
5. **srv version** {1 | 2}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Router(config)# interface gigabitethernet 0/0/0	Configures an interface type and enters interface configuration mode
Step 4	sip-ua Example: Router(config-if)# sip-ua	Enters SIP UA configuration mode.
Step 5	srv version {1 2} Example: Router(config-sip-ua)# srv version 2	Generates DNS SRV queries in either RFC 2782 or RFC 2052 format. <ul style="list-style-type: none"> • 1 --The query is set to the domain name prefix of protocol.transport. (RFC 2052 style). • 2 --The query is set to the domain name prefix of _protocol._transport. (RFC 2782 style). This is the default.
Step 6	exit Example: Router(config-sip-ua)# exit	Exits the current configuration mode.

Configure DNS Server Lookups

Following is the example to configure '_sip_udp.'

```
!
dial-peer voice 1 voip
  session protocol sipv2
  session transport udp
  session target dns:cisco.com
!
```

Following are the examples to configure '_sip_tcp.'

```
!
dial-peer voice 1 voip
  session protocol sipv2
  session transport tcp
```

```

    session target dns:cisco.com
  !
  !
dial-peer voice 1 voip
  session protocol sipv2
  session transport tcp tls
  session target dns:cisco.com
  !

```

Following is the example to configure '_sips._tcp.'.

```

  !
dial-peer voice 1 voip
  session protocol sipv2
  session transport tcp tls
  session target dns:cisco.com
  voice-class sip url sips
  !

```

From Cisco IOS XE Release 16.12.3 onwards, CUBE sends '_sips._tcp.' query when the transport is TLS. The '_sips._tcp.' query is independent of the URI scheme—sip or sips. Following is the example to configure '_sips._tcp.'.

```

  !
dial-peer voice 1 voip
  session protocol sipv2
  session transport tcp tls
  session target dns:cisco.com
  !

```

Following is the sample configuration for a local DNS SRV.

```

  !
ip name-server 172.18.110.64
  !
ip domain lookup
  !
ip host 1.cisco.com 10.10.10.1
ip host 2.cisco.com 10.10.10.2
ip host 3.cisco.com 10.10.10.3
  !
ip host _sip._tcp.cisco.com srv 1 50 5061 1.cisco.com
ip host _sip._tcp.cisco.com srv 1 50 5061 2.cisco.com
ip host _sip._tcp.cisco.com srv 1 50 5061 3.cisco.com
  !
ip host _sips._tcp.cisco.com srv 1 50 5061 1.cisco.com
ip host _sips._tcp.cisco.com srv 1 50 5061 2.cisco.com
ip host _sips._tcp.cisco.com srv 1 50 5061 3.cisco.com
  !
ip host _sip._udp.cisco.com srv 1 50 5060 1.cisco.com
ip host _sip._udp.cisco.com srv 1 50 5060 2.cisco.com
ip host _sip._udp.cisco.com srv 1 50 5060 3.cisco.com
  !
ip host _sip._tcp.cisco.com srv 1 50 5060 1.cisco.com
ip host _sip._tcp.cisco.com srv 1 50 5060 2.cisco.com
ip host _sip._tcp.cisco.com srv 1 50 5060 3.cisco.com
  !

```

Verifying

The following example shows sample is output from the **show sip-ua status** command used to verify the style of DNS server queries:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 1 (rfc 2052)
```




CHAPTER 33

Mid-call Signaling

- [Overview, on page 331](#)
- [Prerequisites, on page 332](#)
- [Mid-call Signaling Passthrough - Media Change, on page 333](#)
- [Mid-call Signaling Block, on page 336](#)
- [Mid Call Codec Preservation, on page 339](#)

Overview

The Cisco Unified Border Element (CUBE) Mid-call Signaling support aims to reduce the interoperability issues that arise due to consuming mid-call RE-INVITES/UPDATES.

Mid-call Re-INVITES/UPDATES can be consumed in the following ways:

- Mid-call Signaling Passthrough - Media Change
- Mid-call Signaling Block
- Mid-call Signaling Codec Preservation



Note This feature should be used as a last resort only when there is no other option in CUBE. This is because configuring this feature can break video-related features. For Delay-offer Re-INVITE, the configured codec will be passed as an offer in 200 message to change the codec, the transcoder is added in the answer.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 49: Feature Information for Mid-call Signaling

Feature Name	Releases	Feature Information
Mid-call Re-INVITE Consumption	Cisco IOS XE 3.6S	The Mid-call Re-INVITE consumption feature consumes mid-call Re-INVITEs from CUBE and helps to avoid interoperability issues because of these re-invites The following commands were introduced or modified: midcall-signaling .
Mid-call Codec Preservation	Cisco IOS XE 3.9S	The Mid-call Codec Preservation feature helps to disables codec negotiation in the middle of a call and preserves the codec negotiated before the call. The following commands were introduced or modified: midcall-signaling preserve-codec , voice-class sip midcall-signaling preserve-codec .
Mid-call Re-INVITE Consumption Enhancements	Cisco IOS XE 3.16S	Mid-call signaling Re-INVITE consumption is enhanced to support: <ul style="list-style-type: none"> • Re-INVITE based call transfer • Call transfer with REFER Consume • Normalization of call hold in a call set-up

Prerequisites

Enable CUBE application on a device

Mid-call Signaling Passthrough - Media Change

Passthrough media change method optimizes or consumes mid-call, media-related signaling within the call. Mid-call signaling changes will be passed through only when bidirectional media like T.38 or video is added. The command **midcall-signaling passthru media-change** needs to be configured to enable passthrough media change.

Restrictions

- Session Description Protocol (SDP) -passthrough is not supported.
- When **codec T** is configured, the offer from CUBE has only audio codecs, and so the video codecs are not consumed.
- Re-invites are not consumed if media flow-around is configured.
- Re-invites are not consumed if media anti-tromboning is configured.
- De-escalation re-invites are consumed. So, one call leg might be de-escalated to audio only while the other call leg continues to support audio and video.
- Re-invites with media direction changes are consumed.
- Video transcoding is not supported.
- Multicast Music On Hold (MMOH) is not supported.
- When the **midcall-signaling passthru media-change** command is configured transcoder is enabled, there might be some impact on Digital Signal Processing (DSP) resources as the transcoder might be used for all the calls.
- Session timer is handled leg by leg whenever this feature is configured and it includes session timer negotiation for initial INVITE/200 OK transaction as well.
- More than two m-lines in the SDP is not supported.
- Alternative Network Address Types (ANAT) is not supported.
- Video calls and Application streams are not supported when mid-call signaling block is configured.
- In the SRTP-RTP scenario, re-invites are not consumed.

Behavior of Mid-call Re-INVITE Consumption

- If mid-call signaling block is enabled on either of call-legs, video parameters and application streams are not negotiated, and are rejected in the answer.
- When flow around and offer-all is configured, CUBE performs codec renegotiation even if mid-call signaling block is configured globally.
- The following behavior is for refer consume scenario:
 - REFER consume is supported for blind, alert and consult call transfers.

- Existing codecs or DTMF is used for local bridging of new call legs. No Re-INVITE or UPDATE is sent for media re-negotiation after REFER.
 - Call gets dropped when DSP is required but not available.
 - A call can be escalated to video only if transferee and transfer-to dial-peers do not have mid-call signaling block configured.
 - Video calls are de-escalated if mid-call signaling block configuration on transfer-to dial-peer.
 - For Re-INVITE based call-transfer involving Cisco Unified Communications Manager, all Re-INVITE are locally answered and transcoder is invoked if negotiated codecs are different than the codecs before call-transfer.
- The following behavior is for INVITE with REPLACES Header consume scenario:
 - CUBE consumes INVITE with REPLACES Header only when the **handle-replaces** CLI is configured (under **sip-ua** or **voice-class tenant**). In this case, CUBE consumes the INVITE and handles it locally. It triggers an outbound INVITE without replaces header and call gets connected with agent.
 - If the **handle-replaces** CLI is enabled, the 'transfer-to' party must have the same codec that is used for the original call setup. If there is a different codec offer, CUBE rejects the INVITE with 488 error.
 - If the **handle-replaces** CLI is not configured, CUBE does not consume the INVITE with REPLACES Header and the outgoing INVITE holds same replace header which CUBE is received.
 - INVITE with REPLACES Header consumption does not support the following configurations:
 - Delayed Offer INVITE
 - Codec, DTMF attribute changes, and RSVP
 - Mid-call Signaling block
 - IPv6
 - The following table provides the details of the behavior when the initial call is establish without 'sendrecv' parameter, that means, the initial call is established with 'sendonly', 'recvonly' or 'inactive'.

Scenario	Behavior
If an Offer is received with 'sendonly' and mid-call block is configured on any or both call legs	Offer is sent with 'sendrecv'.
If an Answer is received with 'sendonly' and the peer leg supports mid-call signaling	Answer is sent with 'sendonly'. Resume transaction is end-to-end.
If an Answer is received with 'sendonly' and the peer leg does not supports mid-call signaling	Answer is sent with 'sendrecv'. Resume transaction is consumed.
If Offer as well as Answer is received with 'sendonly' and Offering leg does not support mid-call signaling	Answer is sent with 'recvonly'. Resume from Offering leg is end-to-end. Resume from answering leg is consumed.

Scenario	Behavior
If Offer as well as Answer is received with 'sendonly' and Answering leg does not support mid-call signaling	Answer is sent with 'inactive'. Resume from Offering leg is consumed. Resume from answering leg is end-to-end.
If Offer as well as Answer is received with 'sendonly' and both legs do not support mid-call signaling	Answer is sent with 'recvonly'. Resume transaction is consumed.

Configure Passthrough of Mid-call Signalling

Perform this task to configure passthrough of mid-call signaling (as Re-invites) only when bidirectional media is added.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure passthrough of mid-call signaling changes only when bidirectional media is added.
 - In Global VoIP SIP configuration mode
 - midcall-signaling passthru media-change**
 - In dial-peer configuration mode
 - voice-class sip midcall-signaling passthru media-change**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Configure passthrough of mid-call signaling changes only when bidirectional media is added. <ul style="list-style-type: none"> • In Global VoIP SIP configuration mode <ul style="list-style-type: none"> midcall-signaling passthru media-change • In dial-peer configuration mode <ul style="list-style-type: none"> voice-class sip midcall-signaling passthru media-change 	Re-Invites are passed through only when bidirectional media is added.

	Command or Action	Purpose
	<p>Example:</p> <p>In Global VoIP SIP configuration mode:</p> <pre>Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# midcall-signaling passthru media-change</pre> <p>Example:</p> <p>In Dial-peer configuration mode:</p> <pre>Device(config)# dial-peer voice 2 voip Device(config-dial-peer)# voice-class sip midcall-signaling passthru media-change</pre>	
Step 4	end	Exits to privileged EXEC mode.

Example Configuring Passthrough SIP Messages at Dial Peer Level

The following example shows how to passthrough SIP messages at the dial peer Level:

```
dial-peer voice 600 voip
destination-pattern 222222222
session protocol sipv2
session target ipv4:9.45.38.39:9001
voice-class sip midcall-signaling passthru media-change
incoming called-number 111111111
voice-class codec 2 offer-all
dial-peer voice 400 voip
destination-pattern 111111111
session protocol sipv2
session target ipv4:9.45.38.39:9000
incoming called-number 222222222
voice-class codec 1 offer-all
```

Example Configuring Passthrough SIP Messages at the Global Level

The following example shows how to passthrough SIP messages at the global level:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# midcall-signaling passthru media-change
```

Mid-call Signaling Block

The Block method blocks all mid-call media-related signaling to the specific SIP trunk. The command **midcall-signaling block** needs to be configured to enable this behavior. Video escalation and T.38 call flow are rejected when the **midcall-signaling block** command is configured. This command should be configured only when basic call is the focus and mid-call can be consumed.

Restrictions

- Session Description Protocol (SDP) -passthrough is not supported
- Video calls and Application streams are not supported.
- When media flow-around is configured, Mid-call INVITE is rejected with 488 error message.
- Re-invites are not consumed if media anti-tromboning is configured.
- Multicast Music On Hold (MMOH) is not supported.
- When the **midcall-signaling passthru media-change** command is configured transcoder is enabled, there might be some impact on Digital Signal Processing (DSP) resources as the transcoder might be used for all the calls.
- Session timer is handled leg by leg whenever this feature is configured.
- More than two m-lines in the SDP is not supported.
- Alternative Network Address Types (ANAT) is not supported.
- When mid-call signaling block is configured, you can either configure REFER consume or enable TCL script. Mid-call signaling block is not supported if both REFER consume and TCL script are enabled. We also recommend not to configure **supplementary-service media-renegotiate** command.
- In the SRTP-RTP scenario, re-invites are not consumed.

Blocking Mid-Call Signaling

Perform this task to block mid-call signaling:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure blocking of mid-call signaling changes:
 - In Global VoIP SIP configuration mode
 - midcall-signaling block**
 - In dial-peer configuration mode
 - voice-class sip midcall-signaling block**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Configure blocking of mid-call signaling changes: <ul style="list-style-type: none"> • In Global VoIP SIP configuration mode midcall-signaling block • In dial-peer configuration mode voice-class sip midcall-signaling block Example: In Global VoIP SIP configuration mode: Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# midcall-signaling block Example: In Dial-peer configuration mode: Device(config)# dial-peer voice 2 voip Device(config-dial-peer)# voice-class sip midcall-signaling block	Mid-call signaling is always blocked.
Step 4	end	Exits to privileged EXEC mode.

Example Blocking SIP Messages at Dial Peer Level

```
dial-peer voice 107 voip
 destination-pattern 74000
 session protocol sipv2
 session target ipv4:9.45.36.9
 incoming called-number 84000
 voice-class codec 1 offer-all
!
dial-peer voice 110 voip
 destination-pattern 84000
 session protocol sipv2
 session target ipv4:9.45.35.2
 incoming called-number 74000
 voice-class codec 1 offer-all
 voice-class sip midcall-signaling block
!
```

Example: Blocking SIP Messages at the Global Level

The following example shows how to block SIP messages at the global Level

```
Device(config)#voice service voip
Device(config-voi-serv)#no ip address trusted authenticate
Device(config-voi-serv)#allow-connections sip to sip
Device(config-voi-serv)#sip
Device(config-serv-sip)#midcall-signaling block
```

Mid Call Codec Preservation

Mid call codec preservation defines whether a codec can be negotiated after a call has been initiated. You can enable or disable codec negotiation in the middle of a call.

Configure Mid Call Codec Preservation

This task disables codec negotiation in the middle of a call and preserves the codec negotiated before the call.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following to disable midcall codec renegotiation:
 - In Global VoIP SIP configuration mode


```
midcall-signaling preserve-codec
```
 - In dial-peer configuration mode


```
voice-class sip midcall-signaling preserve-codec
```
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following to disable midcall codec renegotiation: <ul style="list-style-type: none"> • In Global VoIP SIP configuration mode <pre>midcall-signaling preserve-codec</pre> • In dial-peer configuration mode <pre>voice-class sip midcall-signaling preserve-codec</pre> Example: Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# midcall-signaling preserve-codec	Disables codec negotiation in the middle of a call and preserves the codec negotiated before the call.

Example: Configuring Mid Call Codec Preservation at the Dial Peer Level

	Command or Action	Purpose
	Example: Device(config)# dial-peer voice 10 voip Device(conf-dial-peer)# voice-class sip midcall-signaling preserve-codec	
Step 4	end Example: Device(conf-serv-sip)# end	Exits to privileged EXEC mode.

Example: Configuring Mid Call Codec Preservation at the Dial Peer Level

```

dial-peer voice 107 voip
 destination-pattern 74000
 session protocol sipv2
 session target ipv4:9.45.36.9
 incoming called-number 84000
 voice-class codec 1 offer-all
!
dial-peer voice 110 voip
 destination-pattern 84000
 session protocol sipv2
 session target ipv4:9.45.35.2
 incoming called-number 74000
 voice-class codec 1 offer-all
 voice-class sip midcall-signaling preserve-codec
!

```

Example: Configuring Mid Call Codec Preservation at the Global Level

```

Device(config)# voice service voip
Device(conf-voi-serv)# no ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# midcall-signaling preserve-codec

```



CHAPTER 34

Early Dialog UPDATE Block

- [Overview, on page 341](#)
- [Important Characteristics of Early Dialog UPDATE Block, on page 342](#)
- [Prerequisites, on page 343](#)
- [Restrictions, on page 343](#)
- [Configure Early Dialog UPDATE Block, on page 343](#)
- [Configure Early Dialog UPDATE Block Renegotiate, on page 344](#)
- [Tips to Troubleshoot, on page 345](#)

Overview

This feature enables Cisco Unified Border Element (CUBE) to consume UPDATE requests with SDP, received during an early dialog. UPDATE requests are blocked at CUBE and are not passed through from one leg to the other leg.

If the UPDATE request contains changes in caller-ID, transcoder insertion or deletion, or video escalation or de-escalation, then, CUBE can renegotiate the capabilities by sending a DO re-invite after the call is established.

UPDATE request with SDP received during an early dialog is consumed by CUBE and hence is not passed from one leg to the other leg. This feature can be configured only for the UPDATE requests with SDP.

To pass through the information in UPDATE requests containing changes in caller-ID, transcoder insertion or deletion, or video escalation or de-escalation, CUBE can renegotiate the capabilities by sending a DO re-invite after the call is established. Thus both the user agents are synchronized and this helps in effective utilization of resources.

Renegotiation can be configured only for the UPDATE requests containing the following changes:

- Caller ID
- Transcoder insertion or deletion
- Video escalation or de-escalation

Feature Information

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 50: Feature Information for Mid-call Signaling

Feature Name	Releases	Feature Information
Early Dialog UPDATE Block	Cisco IOS XE 3.16S	This feature allows CUBE to consume the UPDATE requests with SDP received during an early dialog. The following command is introduced: early-media update block .

Important Characteristics of Early Dialog UPDATE Block

The following are a few important characteristics of Early Dialog UPDATE block:

- If multiple codec's is offered by the user agent through an UPDATE, first codec common between received and configured in in-leg at dial-peer is sent in 200OK.
- UPDATE request is consumed, if an UPDATE request with SDP is received after CUBE sends out 200 OK for an INVITE and before ACK is received.
- A 200 Ok is sent for an UPDATE even if there is no transcoder available ONLY for DTMF (rtp-n-te to inband). CUBE falls back to inband.
- If Transcoder is unavailable, only the first codec received in the UPDATE request is sent in 200OK.
- CUBE sends 488 message if transcoder is required but unavailable for codec changes.
- When a video escalation is received via UPDATE, CUBE sends 200 OK with video port as ZERO. No Video data plane sessions are created.
- When a video de-escalation is received via UPDATE, CUBE sends 200 ok with video port as ZERO. Data plane sessions for video are made as INACTIVE instead of deleting. So, effectively there will be four 2 DP connections present with remote video port as ZERO.
- Early-media UPDATE renegotiation takes precedence over DO-EO renegotiation.
- If an early dialog UPDATE is received from one leg to change the caller-ID and the other leg supports UPDATE method, CUBE sends across the caller-id UPDATE to other side and there wont be any renegotiation.
- If Re-Invite is received before triggering DO invite, then DO is not triggered.
- If **no update-callerid** command is enabled and UPDATE request contains only caller-ID changes, then re-negotiation does not happen for any early dialog caller-ID changes. If UPDATE request contains transcoder changes or video escalation or de-escalation, re-negotiation happens even if **no update-callerid** command is enabled.
- If mid-call signaling block is configured, DO invite is not triggered.

- If 18x block is enabled, CUBE fails to add rel1xx related fields in the header. 100rel is dependent on 181 sdp block.

Prerequisites

rel1xx require "100rel" command needs to be configured in global voice service voip sip configuration mode.

Restrictions

- Switch over to fax calls are not supported.
- Session Description Protocol (SDP) passthrough is not supported.
- Alternative Network Address Types (ANAT) is not supported.

Configure Early Dialog UPDATE Block

Configuring early dialog UPDATE Block enables CUBE to block all early dialog UPDATE requests from passing through to the user agents.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands to block early dialog UPDATE requests:
 - In the dial-peer configuration mode
voice-class sip early-media update block
 - In the global VoIP SIP configuration mode
early media update block
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands to block early dialog UPDATE requests:	

	Command or Action	Purpose
	<ul style="list-style-type: none"> In the dial-peer configuration mode voice-class sip early-media update block In the global VoIP SIP configuration mode early media update block <p>Example: In dial-peer configuration mode</p> <pre>!Applying Early Dialog UPDATE block to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip early-media update block Device (config-dial-peer)# end</pre> <p>Example: In global VoIP SIP configuration mode</p> <pre>! Applying Early Dialog UPDATE block globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# early media update block Device (config-voi-sip)# end</pre>	
Step 4	end	Exits VoIP SIP configuration mode and enters privileged EXEC mode.

Configure Early Dialog UPDATE Block Renegotiate

Configuring Early Dialog UPDATE Block Renegotiate enables CUBE to renegotiate the call if UPDATE request with SDP contains changes caller-ID, transcoder insertion or deletion, or video escalation or deletion. CUBE renegotiates by sending a DO re-invite after the call is established.

SUMMARY STEPS

- enable**
- configure terminal**
- Enter one of the following commands:
 - In the dial-peer configuration mode
voice-class sip early-media update block re-negotiate
 - In the global VoIP configuration mode
early media update block re-negotiate
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • In the dial-peer configuration mode voice-class sip early-media update block re-negotiate • In the global VoIP configuration mode early media update block re-negotiate <p>Example: In dial-peer configuration mode</p> <pre>!Applying Early Dialog UPDATE block re-negotiate to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip early-media update block re-negotiate Device (config-dial-peer)# end</pre> <p>Example: In global VoIP SIP configuration mode</p> <pre>! Applying Early Dialog UPDATE block re-negotiate globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# early media update block re-negotiate Device (config-voi-sip)# end</pre>	Renegotiates the call if the UPDATE request contains changes in caller ID, transcoder addition or deletion, or video escalation or de-escalation.
Step 4	end	Exits VoIP SIP configuration mode and enters privileged EXEC mode.

Tips to Troubleshoot

Use the following command for debugging information:

- **debug ccsip all**
- **debug voip ccapi inout**
- **show voip rtp connections**



CHAPTER 35

Forked 18x Responses

- [Overview, on page 347](#)
- [Prerequisites, on page 348](#)
- [Restrictions, on page 349](#)
- [Configure Consumption of Forked 18x Responses with SDP During Early Dialog, on page 349](#)
- [Configure Consumption of Forked 18x Responses with SDP During Early Dialog Renegotiate, on page 350](#)
- [Tips to Troubleshoot, on page 351](#)

Overview

The Cisco Unified Border Element (CUBE) supports consumption of forked 18x responses with SDP, under certain conditions during an early dialog, to reduce the interoperability issues that arise due to signaling forking.

When CUBE receives forked 18x responses with SDP, the media negotiation by default is end-to-end. This means that CUBE has to send an UPDATE with SDP on the inbound leg to renegotiate the new media offer. Under certain conditions, the inbound leg may not be able to support sending UPDATE messages with SDP for media renegotiation. This results in CUBE consuming the forked 18x responses with SDP and may result in DSP resources being used for media interworking. Media parameters such as direction change, and call escalation or de-escalation is not propagated end-to-end. If required, these media changes can be renegotiated end-to-end, after the calls are connected, using a DO re-INVITE.

Forked 18x responses for INVITE requests with SDP during early dialog will be consumed by CUBE to reduce interoperability issues between user agents.

Feature Information for Consumption of Multiple Forked 18x Responses with SDP During Early Dialog

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 51: Feature Information for Consumption of Multiple Forked 18x Responses with SDP During Early Dialog

Feature Name	Releases	Feature Information
Support for Forked 18x Responses with SDP during Early Dialog	Cisco IOS XE Denali 16.3.1	This feature allows CUBE to consume multiple forked 18x responses with SDP received during an early dialog.

Characteristics of Forked 18x Responses with SDP during Early Dialog

- If PRACK or UPDATE is not supported on the inbound leg, by default, CUBE consumes the forked 18x responses
- If PRACK or UPDATE is not supported and CUBE has to initiate renegotiation after call connect, then the **early media update block re-negotiate** CLI must be enabled
- When PRACK and UPDATE are supported on the inbound leg and CUBE has to consume the forked 18x responses, the **early media update block** CLI must be enabled
- If PRACK and UPDATE are supported and CUBE has to consume the forked 18x responses and initiate renegotiation after call connect, then the **early media update block renegotiate** CLI must be enabled
- If mid-call signaling block or mid-call signaling passthrough media changes are configured, DO invite is not triggered



Note CUBE utilizes the EARLY UPDATE BLOCK functionality to configure the forked 18x responses with SDP during early dialog. The **early media update block** command is used to consume the forked 18x responses and the **early media update block renegotiate** command is used to renegotiate the forked 18x responses after the call connect.

Renegotiation (when enabled via configuration) is triggered for the forked 18x responses containing the following changes:

- DSP Transcoder insertion
- Video escalation or de-escalation
- Media directional changes



Note It is recommended to configure the **early media update block re-negotiate** command whenever there are transcoding, DTMF interworking, or video changes.

Prerequisites

- Re-negotiation is triggered only if the renegotiate **early media update block re-negotiate** CLI is enabled

Restrictions

The following features or call-flows are not supported:

- SIP Delayed-Offer to Delayed-Offer call flows
- Session Description Protocol (SDP) passthrough mode
- Secure Real-Time Transport Protocol (SRTP) passthrough calls
- Alternative Network Address Types (ANAT)
- Media flow-around
- Media anti-trombone
- Early-dialog UPDATE block

Configure Consumption of Forked 18x Responses with SDP During Early Dialog

Perform the following procedure to enable CUBE to block all early dialog forked 18x requests from passing through to the user agents.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands to block the forked 18x responses with SDP during early dialog:
 - In the dial-peer configuration mode
voice-class sip early-media update block
 - In the global VoIP SIP configuration mode
early media update block
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands to block the forked 18x responses with SDP during early dialog:	

	Command or Action	Purpose
	<ul style="list-style-type: none"> In the dial-peer configuration mode voice-class sip early-media update block In the global VoIP SIP configuration mode early media update block <p>Example: In dial-peer configuration mode</p> <pre>!Applying Early Dialog UPDATE block to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip early-media update block Device (config-dial-peer)# end</pre> <p>Example: In global VoIP SIP configuration mode</p> <pre>! Applying Early Dialog UPDATE block globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# early media update block Device (config-voi-sip)# end</pre>	
Step 4	end	Exits VoIP SIP configuration mode and enters privileged EXEC mode.

Configure Consumption of Forked 18x Responses with SDP During Early Dialog Renegotiate

Perform the following procedure to enable CUBE to renegotiate forked 18x calls with SDP during early dialog after consumption of these forked 18x responses. CUBE renegotiates by sending a DO invite after the call is established.

SUMMARY STEPS

- enable**
- configure terminal**
- Enter one of the following commands:
 - In the dial-peer configuration mode
voice-class sip early-media update block re-negotiate
 - In the global VoIP configuration mode
early media update block re-negotiate
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • In the dial-peer configuration mode voice-class sip early-media update block re-negotiate • In the global VoIP configuration mode early media update block re-negotiate <p>Example: In dial-peer configuration mode</p> <pre>!Applying Early Dialog UPDATE block re-negotiate to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip early-media update block re-negotiate Device (config-dial-peer)# end</pre> <p>Example: In global VoIP SIP configuration mode</p> <pre>! Applying Early Dialog UPDATE block re-negotiate globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# early media update block re-negotiate Device (config-voi-sip)# end</pre>	Renegotiates the call if the forked 18x responses with SDP during early dialog contains changes in transcoder addition, or video escalation or de-escalation.
Step 4	end	Exits VoIP SIP configuration mode and enters privileged EXEC mode.

Tips to Troubleshoot

Use the following command for debugging information:

- debug ccsip verbose
- show voip rtp connections detail
- show call active voice brief
- show dspfarm dsp active

- show voice dsmp stream brief
- show platform hardware qfp active feature sbc global



CHAPTER 36

Pass-Through of Unsupported Content Types in SIP INFO Messages

- [Overview, on page 353](#)
- [Feature Information , on page 354](#)
- [Configure to Pass-through All Unsupported Content Types in a SIP INFO Messages, on page 354](#)

Overview

This feature allows the CUBE to pass-through all unsupported content types in a SIP INFO message.

The Support for Pass-Through of Unsupported Content Types in SIP INFO Messages feature allows the CUBE to pass-through all unsupported content types in a SIP INFO message.

Upon receipt of a SIP INFO message with unsupported content type, CUBE triggers a SIP INFO message on the outgoing peer call leg. The response received for this SIP INFO message is triggered on the incoming peer call leg and information flows end-to-end.

Supported content types include the following:

- application/sdp
- application/qsig
- application/media-control+xml
- application/x-q931
- application/gtd
- application/simple-message-summary
- application/kpml-response+xml
- application/dtmf-relay
- application/broadsoft
- message/sipfrag
- audio/telephone-event
- multipart/mixed

- application/x-cisco-record+json

Feature Information

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 <https://cfmg.cisco.com/>. An account on Cisco.com is not required.

Feature Name	Releases	Feature Information
Support for pass-through of unsupported content types in SIP INFO messages	Baseline functionality	This feature allows CUBE to pass-through SIP INFO methods or request message types with unsupported content types. Media negotiation and media exchange is completely end-to-end.

Configure to Pass-through All Unsupported Content Types in a SIP INFO Messages

You must enable the **pass-thru content un supp** command to pass-through all unsupported content types in a SIP INFO message. There is no additional configuration task required for this feature.



CHAPTER 37

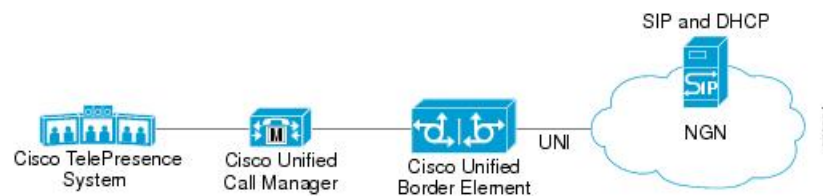
Support for PAID, PPID, Privacy, PCPID, and PAURI Headers

- [Overview, on page 355](#)
- [Restrictions, on page 365](#)
- [Configure P-Header and Random-Contact Support , on page 366](#)

Overview

The figure below shows a typical network topology where the Cisco Unified Border Element (CUBE) is configured to route messages between a call manager system (such as the Cisco Unified Call Manager) and a Next Generation Network (NGN).

Figure 31: Cisco Unified Border Element and Next Generation Topology



Devices that connect to an NGN must comply with the User-Network Interface (UNI) specification. The CUBE supports the NGN UNI specification and can be configured to interconnect NGN with other call manager systems, such as the Cisco Unified Call Manager.

The CUBE supports the following:

- the use of P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID), in INVITE messages
- the translation of PAID headers to PPID headers and vice versa
- the translation of RPID headers to PAID or PPID headers and vice versa
- the configuration and/or pass through of privacy header values
- the use of the PCPID header to route INVITE messages
- the use of multiple PAURI headers in the response messages (200 OK) it receives to REGISTER messages

P-Preferred Identity and P-Asserted Identity Headers

NGN servers use the PPID header to identify the preferred number that the caller wants to use. The PPID is part of INVITE messages sent to the NGN. When the NGN receives the PPID, it authorizes the value, generates a PAID based on the preferred number, and inserts it into the outgoing INVITE message towards the called party.

However, some call manager systems, such as Cisco Unified Call Manager 5.0, use the Remote-Party Identity (RPID) value to send calling party information. Therefore, the Cisco Unified Border Element must support building the PPID value for an outgoing INVITE message to the NGN, using the RPID value or the From: value received in the incoming INVITE message. Similarly, CUBE supports building the RPID and/or From: header values for an outgoing INVITE message to the call manager, using the PAID value received in the incoming INVITE message from the NGN.

In non-NGN systems, the CUBE can be configured to translate between PPID and PAID values, and between From: or RPID values and PAID/PPID values, at global and dial-peer levels.

In configurations where all relevant servers support the PPID or PAID headers, the Cisco Unified Border Element can be configured to transparently pass the header.



Note If the NGN sets the From: value to anonymous, the PAID is the only value that identifies the caller.

The table below describes the types of INVITE message header translations supported by the Cisco Unified Border Element. It also includes information on the configuration commands to use to configure P-header translations.

The table below shows the P-header translation configuration settings only. In addition to configuring these settings, you must configure other system settings (such as the session protocol).

Table 52: P-header Configuration Settings

Incoming Header	Outgoing Header	Configuration Notes
From:	RPID	To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# remote-party-id This is the default system behavior. Note If both, remote-party-id and asserted-id commands are configured, then the asserted-id command takes precedence over the remote-part-id command.
PPID	PAID	To enable the translation to PAID privacy headers in the outgoing header at a global level, use the asserted-id pai command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# asserted-id pai To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id pai command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id pai

Incoming Header	Outgoing Header	Configuration Notes
PPID	RPID	To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# remote-party-id This is the default system behavior.
PAID	PPID	To enable the translation to PPID privacy headers in the outgoing header at a global level, use the asserted-id ppi command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# asserted-id ppi To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id ppi command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id ppi
PAID	RPID	To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# remote-party-id This is the default system behavior.
RPID	PPID	To enable the translation to PPID privacy headers in the outgoing header at a global level, use the asserted-id ppi command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# asserted-id ppi To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id ppi command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id ppi
RPID	PAID	To enable the translation to PAID privacy headers in the outgoing header at a global level, use the asserted-id pai command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# asserted-id pai To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id pai command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id pai
RPID	From:	By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the no remote-party-id command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# no remote-party-id



Note Privacy functions are not initialized on Unified Border Element without configuring **asserted-id pai** or **asserted-id ppi**. Ensure that you configure **asserted-id pai** or **asserted-id ppi** to support privacy functions on Unified Border Element.

Just configuring **asserted-id pai** in dial-peer or global configuration mode is sufficient to process both PPID and PAID headers.

The CUBE can be configured to transparently pass the PAID and PPID headers in the incoming and outgoing Session Initiation Protocol (SIP) requests or response messages from end-to-end.

- Requests include: INVITEs and UPDATEs
- Responses include: 18x and 200OK



Note The priority of P-headers are in the following order: PAID, PPID, and RPID.

Table 53: PAID and PPID header configuration settings for mid-call requests and responses

Incoming Header	Outgoing Header	Configuration Notes
PAID	PPID	<p>To enable the translation to PPID headers in the outgoing header at a global level, use the asserted-id ppi command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# asserted-id ppi</p> <p>To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id ppi command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id ppi</p>

Incoming Header	Outgoing Header	Configuration Notes
RPID	PPID	<p>To enable the translation to PPID headers in the outgoing header at a global level, use the asserted-id ppi command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# asserted-id ppi</p> <p>To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id ppi command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id ppi</p>
PPID	PPID	<p>To enable the translation to PPID headers in the outgoing header at a global level, use the asserted-id ppi command in voice service VoIP SIP configuration mode.</p> <p>To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id ppi command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id ppi</p>
PAID	PAID	<p>To enable the translation to PAID headers in the outgoing header at a global level, use the asserted-id pai command in voice service VoIP SIP configuration mode.</p> <p>To enable the translation to PAID headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id pai command in dial peer voice configuration mode. For example: Router(config-dial-peer)# voice-class sip asserted-id pai</p>

Incoming Header	Outgoing Header	Configuration Notes
RPID	PAID	<p>To enable the translation to PAID headers in the outgoing header at a global level, use the asserted-id pai command in voice service VoIP SIP configuration mode.</p> <p>To enable the translation to PAID headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id pai command in dial peer voice configuration mode.</p>
PPID	PAID	<p>To enable the translation to PAID headers in the outgoing header at a global level, use the asserted-id pai command in voice service VoIP SIP configuration mode.</p> <p>To enable the translation to PAID headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id pai command in dial peer voice configuration mode.</p>
PAID	RPID	<p>To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example:</p> <pre>Router(config-sip-ua)# remote-party-id.</pre> <p>Note PAID and PPID headers are not configured in this case.</p>
RPID	RPID	<p>To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example:</p> <pre>Router(config-sip-ua)# remote-party-id.</pre> <p>Note PAID and PPID headers are not configured in this case.</p>

Incoming Header	Outgoing Header	Configuration Notes
PPID	RPID	To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# remote-party-id
FROM	FROM	No configuration required except for the remote-party-id header.
FROM	RPID	To enable the translation to RPID headers in the outgoing header, use the remote-party-id command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# remote-party-id
PAID	PAID	Enables PPID headers on the incoming dial-peer and PAID headers on the outgoing dial-peer.
RPID	PAID	Enables PPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PPID	PAID	Enables PPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PAID	PAID	Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
RPID	PAID	Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PPID	PAID	Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PAID	PPID	Enables PAID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
RPID	PPID	Enables PAID headers on incoming dial-peer and PPID headers on outgoing dial-peer.

Incoming Header	Outgoing Header	Configuration Notes
PPID	PPID	Enables PAID headers on incoming dial-peer and PPID on outgoing dial-peer.
PAID	PPID	Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
RPID	PPID	Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
PPID	PPID	Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
PAID	RPID	Enables PPID headers on incoming dial-peer and RPID headers on outgoing dial-peer. Note PAID headers will be given priority and RPID headers will be created using the PAID header information.
RPID	RPID	Enables PPID headers on incoming dial-peer and RPID headers on outgoing dial-peer.
PPID	RPID	Enables PPID headers on incoming dial-peer and RPID headers on outgoing dial-peer. Note PPID headers will be given priority and RPID headers will be created using the PPID header information.
PAID	RPID	Enables PAID headers on incoming dial-peer and RPID headers on outgoing dial-peer. Note PAID headers will be given priority and RPID headers will be created using the PAID header information.

Incoming Header	Outgoing Header	Configuration Notes
RPID	RPID	Enables PAID headers on incoming dial-peer and RPID headers on outgoing dial-peer.
PPID	RPID	Enables PAID headers on incoming dial-peer and RPID headers on outgoing dial-peer. Note PPID headers will be given priority and RPID headers will be created using the PPID header information.

Privacy

If the user is subscribed to a privacy service, the Cisco Unified Border Element can support privacy using one of the following methods:

- Using prefixes

The NGN dial plan can specify prefixes to enable privacy settings. For example, the dial plan may specify that if the caller dials a prefix of 184, the calling number is not sent to the called party.

The dial plan may also specify that the caller can choose to send the calling number to the called party by dialing a prefix of 186. Here, the Cisco Unified Border Element transparently passes the prefix as part of the called number in the INVITE message.

The actual prefixes for the network are specified in the dial plan for the NGN, and can vary from one NGN to another.

- Using the Privacy header

If the Privacy header is set to None, the calling number is delivered to the called party. If the Privacy header is set to a Privacy:id value, the calling number is not delivered to the called party.

- Using Privacy values from the peer call leg

If the incoming INVITE has a Privacy header or a RPID with privacy on, the outgoing INVITE can be set to Privacy: id. This behavior is enabled by configuring **privacy pstn** command globally or **voice-class sip privacy pstn** command on the selected dial-peer.

Incoming INVITE can have multiple privacy header values, id, user, session, and so on. Configure the **privacy-policy passthru** command globally or **voice-class sip privacy-policy passthru** command to transparently pass across these multiple privacy header values.

Some NGN servers require a Privacy header to be sent even though privacy is not required. In this case the Privacy header must be set to none. The Cisco Unified Border Element can add a privacy header with the value None while forwarding the outgoing INVITE to NGN. Configure the **privacy-policy send-always** globally or **voice-class sip privacy-policy send-always** command in dial-peer to enable this behavior.

If the user is not subscribed to a privacy service, the Cisco Unified Border Element can be configured with no Privacy settings.



Note For the Privacy functions to work as intended, the command **asserted-id {pai|ppi}** must be configured.

P-Called Party Identity

The Cisco Unified Border Element can be configured to use the PCPID header in an incoming INVITE message to route the call, and to use the PCPID value to set the To: value of outgoing INVITE messages.

The PCPID header is part of the INVITE messages sent by the NGN, and is used by Third Generation Partnership Project (3GPP) networks. The Cisco Unified Border Element uses the PCPID from incoming INVITE messages (from the NGN) to route calls to the Cisco Unified Call Manager.



Note The PCPID header supports the use of E.164 numbers only.

P-Associated URI

The Cisco Unified Border Element supports the use of PAURI headers sent as part of the registration process. After the Cisco Unified Border Element sends REGISTER messages using the configured E.164 number, it receives a 200 OK message with one or more PAURIs. The number in the first PAURI (if present) must match the contract number. The Cisco Unified Border Element supports a maximum of six PAURIs for each registration.



Note The Cisco Unified Border Element performs the validation process only when a PAURI is present in the 200 OK response.

The registration validation process works as follows:

- The Cisco Unified Border Element receives a REGISTER response message that includes PAURI headers that include the contract number and up to five secondary numbers.
- The Cisco Unified Border Element validates the contract number against the E.164 number that it is registering:
 - If the values match, the Cisco Unified Border Element completes the registration process and stores the PAURI value. This allows administration tools to view or retrieve the PAURI if needed.
 - If the values do not match, the Cisco Unified Border Element unregisters and then reregisters the contract number. The Cisco Unified Border Element performs this step until the values match.

Random Contact Support

The Cisco Unified Border Element can use random-contact information in REGISTER and INVITE messages so that user information is not revealed in the contact header.

To provide random contact support, the Cisco Unified Border Element performs SIP registration based on the random-contact value. The Cisco Unified Border Element then populates outgoing INVITE requests with the random-contact value and validates the association between the called number and the random value in

the Request-URI of the incoming INVITE. The Cisco Unified Border Element routes calls based on the PCPID, instead of the Request-URI which contains the random value used in contact header of the REGISTER message.

The default contact header in REGISTER messages is the calling number. The Cisco Unified Border Element can generate a string of 32 random alphanumeric characters to replace the calling number in the REGISTER contact header. A different random character string is generated for each pilot or contract number being registered. All subsequent registration requests will use the same random character string.

The Cisco Unified Border Element uses the random character string in the contact header for INVITE messages that it forwards to the NGN. The NGN sends INVITE messages to the Cisco Unified Border Element with random-contact information in the Request URI. For example: INVITE sip:FefhH3zIHe9i8ImcGjDD1PEc5XfFy51G@10.12.1.46:5060.

The Cisco Unified Border Element will not use the To: value of the incoming INVITE message to route the call because it might not identify the correct user agent if supplementary services are invoked. Therefore, the Cisco Unified Border Element must use the PCPID to route the call to the Cisco Unified Call Manager. You can configure routing based on the PCPID at global and dial-peer levels.

Feature Information

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 54: Feature Information for PAID and PPID Headers on CUBE

Feature Name	Releases	Feature Information
PAID and PPID Headers in mid-call re-INVITE and UPDATE request and responses on Cisco Unified Border Element	Baseline Fuctionality	This feature enables CUBE platforms to support: <ul style="list-style-type: none"> • P-Preferred Identity (PPID) and P-Asserted Identity (PAID) in mid-call re-INVITE messages and responses from end-to-end. • P-Preferred Identity (PPID) and P-Asserted Identity (PAID) in mid-call UPDATE messages and responses from end-to-end. • Configuration and/or pass through of PAID and PPID header values.

Restrictions

- To enable random-contact support, you must configure the Cisco Unified Border Element to support SIP registration with random-contact information. In addition, you must configure random-contact support in VoIP voice-service configuration mode or on the dial peer.

- If random-contact support is configured for SIP registration only, the system generates the random-contact information, includes it in the SIP REGISTER message, but does not include it in the SIP INVITE message.
- If random-contact support is configured in VoIP voice-service configuration mode or on the dial peer only, no random contact is sent in either the SIP REGISTER or INVITE message.
- Passing of "+" is not supported with PAID PPID Privacy PCPID and PAURI Headers.

Configure P-Header and Random-Contact Support

To enable random contact support you must configure the CUBE to support Session Initiation Protocol (SIP) registration with random-contact information, as described in this section.

To enable the CUBE to use the PCPID header in an incoming INVITE message to route the call, and to use the PCPID value to set the To: value of outgoing INVITE messages, you must configure P-Header support as described in this section.

Configure P-Header Translation

To configure P-Header translations on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **asserted-id header-type**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Router(config)# voice service voip	Enters VoIP voice-service configuration mode.

	Command or Action	Purpose
Step 4	sip Example: Router(conf-voi-serv)# sip	Enters voice service VoIP SIP configuration mode.
Step 5	asserted-id <i>header-type</i> Example: Router(conf-serv-sip)# asserted-id ppi	Specifies the type of privacy header in the outgoing SIP requests and response messages.
Step 6	exit Example: Router(conf-serv-sip)# exit	Exits the current mode.

Configure P-Header Translation on an Individual Dial Peer

To configure P-Header translation on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *tag* voip**
4. **voice-class sip asserted-id *header-type***
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>tag</i> voip Example: Router(config)# dial-peer voice 2611 voip	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 4	voice-class sip asserted-id <i>header-type</i> Example: <pre>Router(config-dial-peer)# voice-class sip asserted-id ppi</pre>	Specifies the type of privacy header in the outgoing SIP requests and response messages, on this dial peer.
Step 5	exit Example: <pre>Router(config-dial-peer)# exit</pre>	Exits the current mode.

Configure P-Called-Party-Id Support

To configure P-Called-Party-Id support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call-route p-called-party-id**
6. **random-request-uri validate**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Router(config)# voice service voip</pre>	Enters VoIP voice-service configuration mode.
Step 4	sip Example:	Enters voice service VoIP SIP configuration mode.

	Command or Action	Purpose
	<code>Router(conf-voi-serv)# sip</code>	
Step 5	call-route p-called-party-id Example: <code>Router(conf-serv-sip)# call-route p-called-party-id</code>	Enables the routing of calls based on the PCPID header.
Step 6	random-request-uri validate Example: <code>Router(conf-serv-sip)# random-request-uri validate</code>	Enables the validation of the random string in the Request URI of the incoming INVITE message.
Step 7	exit Example: <code>Router(conf-serv-sip)# exit</code>	Exits the current mode.

Configure P-Called-Party-Id Support on an Individual Dial Peer

To configure P-Called-Party-Id support on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip call-route p-called-party-id**
5. **voice-class sip random-request-uri validate**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <code>Router# configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	dial-peer voice tag voip Example: Router(config)# dial-peer voice 2611 voip	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	voice-class sip call-route p-called-party-id Example: Router(config-dial-peer)# voice-class sip call-route p-called-party-id	Enables the routing of calls based on the PCPID header on this dial peer.
Step 5	voice-class sip random-request-uri validate Example: Router(config-dial-peer)# voice-class sip random-request-uri validate	Enables the validation of the random string in the Request URI of the incoming INVITE message on this dial peer.
Step 6	exit Example: Router(config-dial-peer)# exit	Exits the current mode.

Configure Privacy Support on a Cisco Unified Border Element

To configure privacy support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. privacy *privacy-option*
6. privacy-policy *privacy-policy-option*
7. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Router# configure terminal	
Step 3	voice service voip Example: Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	sip Example: Router(conf-voi-serv)# sip	Enters voice service VoIP SIP configuration mode.
Step 5	privacy privacy-option Example: Router(conf-serv-sip)# privacy id	Enables the privacy settings for the header.
Step 6	privacy-policy privacy-policy-option Example: Router(conf-serv-sip)# privacy-policy passthru	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next.
Step 7	exit Example: Router(conf-serv-sip)# exit	Exits the current mode.

Configure Privacy Support on an Individual Dial Peer

To configure privacy support on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip privacy privacy-option**
5. **voice-class sip privacy-policy privacy-policy-option**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Router(config)# dial-peer voice 2611 voip	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	voice-class sip privacy privacy-option Example: Router(config-dial-peer)# voice-class sip privacy id	Enables the privacy settings for the header on this dial peer.
Step 5	voice-class sip privacy-policy privacy-policy-option Example: Router(config-dial-peer)# voice-class sip privacy-policy passthru	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next, on this dial peer.
Step 6	exit Example: Router(config-dial-peer)# exit	Exits the current mode.

Configure Random-Contact Support on a Cisco Unified Border Element

To configure random-contact support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. credentials username *username* password *password* realm *domain-name*
5. registrar ipv4: *destination-address* random-contact expires *expiry*
6. exit
7. voice service voip
8. sip
9. random-contact
10. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	sip-ua Example: <pre>Router(config)# sip-ua</pre>	Enters SIP user-agent configuration mode.
Step 4	credentials username <i>username</i> password <i>password</i> realm <i>domain-name</i> Example: <pre>Router(config-sip-ua)# credentials username 123456 password cisco realm cisco</pre>	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	registrar ipv4: <i>destination-address</i> random-contact expires <i>expiry</i> Example: <pre>Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200</pre>	Enables the SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar. <ul style="list-style-type: none"> • The random-contact keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.
Step 6	exit Example: <pre>Router(config-sip-ua)# exit</pre>	Exits the current mode.
Step 7	voice service voip Example: <pre>Router(config)# voice service voip</pre>	Enters VoIP voice-service configuration mode.
Step 8	sip Example: <pre>Router(conf-voi-serv)# sip</pre>	Enters voice service VoIP SIP configuration mode.

	Command or Action	Purpose
Step 9	random-contact Example: <pre>Router(conf-serv-sip)# random-contact</pre>	Enables random-contact support on a Cisco Unified Border Element.
Step 10	exit Example: <pre>Router(conf-serv-sip)# exit</pre>	Exits the current mode.

Configure Random-Contact Support for an Individual Dial Peer

To configure random-contact support for an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **credentials username *username* password *password* realm *domain-name***
5. **registrar ipv4: *destination-address* random-contact expires *expiry***
6. **exit**
7. **dial-peer voice *tag* voip**
8. **voice-class sip random-contact**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	sip-ua Example: <pre>Router(config)# sip-ua</pre>	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 4	credentials username <i>username</i> password <i>password</i> realm <i>domain-name</i> Example: <pre>Router(config-sip-ua)# credentials username 123456 password cisco realm cisco</pre>	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	registrar ipv4: <i>destination-address</i> random-contact expires <i>expiry</i> Example: <pre>Router(config-sip-ua)# registrar ipv4:10.1.1.2.2 random-contact expires 200</pre>	Enables the SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar. <ul style="list-style-type: none"> • The random-contact keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.
Step 6	exit Example: <pre>Router(config-sip-ua)# exit</pre>	Exits the current mode.
Step 7	dial-peer voice <i>tag</i> voip Example: <pre>Router(config)# dial-peer voice 2611 voip</pre>	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 8	voice-class sip random-contact Example: <pre>Router(config-dial-peer)# voice-class sip random-contact</pre>	Enables random-contact support on this dial peer.
Step 9	exit Example: <pre>Router(config-dial-peer)# exit</pre>	Exits the current mode.



CHAPTER 38

Dynamic REFER Handling

- [Dynamic Refer Handling, on page 377](#)
- [Prerequisites, on page 378](#)
- [Restrictions, on page 378](#)
- [Configure REFER Passthrough with Unmodified Refer-To , on page 378](#)
- [REFER Handling - Delayed Disconnect, on page 380](#)
- [Configure REFER Consumption, on page 381](#)
- [Troubleshooting Tips, on page 383](#)

Dynamic Refer Handling

When a dial-peer match occurs, Cisco Unified Border Element (CUBE) passes the REFER message from an in leg to an out leg. Also, the host part of the Refer-to header is modified with the IP address.

The Dynamic REFER handling feature provides configurations to pass across or consume the REFER message. When an endpoint invokes a supplementary service such as a call transfer, the endpoint generates and sends an in-dialog REFER request towards the CUBE. If the REFER message is consumed, an INVITE is sent towards refer-to dial-peer

Feature Information

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 55: Feature Information for Dynamic REFER Handling

Feature Name	Releases	Feature Information
REFER Consume (Enhancements)	Baseline Fuctionality	REFER Consume (Enhancements) provides additional configurations to conditionally forward the REFER message.

Feature Name	Releases	Feature Information
Refer Delay Disconnect	Cisco IOS XE Bengaluru 17.6.1a	Delay disconnect message on transferor leg for REFER transaction.

Prerequisites

Transcoding configuration is required on the CUBE for midcall transcoder insertion, deletion, or modification during call transfers.

Restrictions

- Only Session Initiation Protocol (SIP)-to-SIP call transfers are supported.
- Call escalation and de-escalation are not supported.
- Video transcoding is not supported.
- Session Description Protocol (SDP) pass-through is not supported.
- In REFER consume scenario, if TCL script is enabled, then **supplementary-service media-renegotiate** command should not be configured.

Configure REFER Passthrough with Unmodified Refer-To

This task configures the passthrough of REFER message from the in leg to the out leg on a dial-peer match. A REFER is sent toward inbound dial peer. This task also ensures that the host part of the Refer-to header is unmodified and not changed to the IP address during passthrough.



Note Dataplane session will not be deleted for REFER passthrough scenarios, after receiving REFER message. For Cisco IOS XE Bengaluru 17.6.1a and later, configure **refer-delay-disconnect <secs>**, to override this functionality.

Table 56: Supplementary Service

supplementary service refer	Results
yes	REFER is passed through from the in leg to the out leg.
no	INVITE is sent toward refer-to dial-peer.



Note This configuration in this task can be overridden by the **refer consume** command. Refer to the [Configure REFER Passthrough with Unmodified Refer-To](#) task for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure REFER passthrough:
 - **supplementary-service sip refer** in global VoIP configuration mode.
 - **supplementary-service sip refer** in dial-peer configuration mode.
4. (Optional) Configure unmodified Refer-to:
 - **referto-passing** in Global VoIP SIP configuration mode.
 - **voice-class sip referto-passing [system]** in dial-peer configuration mode.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Configure REFER passthrough: <ul style="list-style-type: none"> • supplementary-service sip refer in global VoIP configuration mode. • supplementary-service sip refer in dial-peer configuration mode. Example: In Global VoIP configuration mode: Device(config)# voice service voip Device(conf-voi-serv)# supplementary-service sip refer Example: In dial-peer configuration mode: Device(config)# dial-peer voice 22 voip	Configures REFER passthrough. A REFER is sent toward the inbound dial peer.

	Command or Action	Purpose
	Device(config-dial-peer)# supplementary-service sip refer	
Step 4	<p>(Optional) Configure unmodified Refer-to:</p> <ul style="list-style-type: none"> • referto-passing in Global VoIP SIP configuration mode. • voice-class sip referto-passing [system] in dial-peer configuration mode. <p>Example:</p> <p>In Global VoIP configuration mode:</p> <pre>Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# referto-passing</pre> <p>Example:</p> <p>In dial-peer configuration mode:</p> <pre>Device(config)# dial-peer voice 22 voip Device(config-dial-peer)# voice-class sip referto-passing</pre>	Ensures that the refer-to header is unmodified and not changed to the IP address during passthrough.
Step 5	end	Exits to privileged EXEC mode.

REFER Handling - Delayed Disconnect

With the current default behaviour of CUBE REFER handling, CUBE disconnects the call on a transferor leg with BYE message, after REFER transaction is successful. Also, CUBE unbridges the media path between transferee and transferor during REFER pass through scenario. This causes the interoperability issues with other third party vendor products wherein the Call Transfer is unsuccessful. To fix this interoperability issues, **refer-delay-disconnect** command is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure refer-delay-disconnect:
 - **refer-delay-disconnect**<1-5>delay value (in seconds) in global VoIP, dial-peer, and tenant configuration modes.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Configure refer-delay-disconnect: <ul style="list-style-type: none"> • refer-delay-disconnect<1-5>delay value (in seconds) in global VoIP, dial-peer, and tenant configuration modes. Example: In Global VoIP configuration mode: <pre>Device(config)# voice service voip Device(conf-voi-serv)#sip Device(conf-serv-sip)#refer-delay-disconnect 3</pre> Example: In dial-peer configuration mode: <pre>Device(config)# dial-peer voice 22 voip Device(config-dial-peer)# voice-class sip refer-delay-disconnect 3</pre> Example: In tenant configuration mode: <pre>Device(config)# voice class tenant 10 Device(config-class)# refer-delay-disconnect 3</pre>	Configures refer-delay-disconnect. Now, CUBE delays the disconnect message (sending BYE) on the transfer leg for the configured timeout.

Configure REFER Consumption

This task configures the consumption of REFER message on a dial-peer match. An INVITE is sent towards the Refer-to dial peer.

Table 57: Configurations for REFER Consumption

supplementary service refer	refer consume	Results
yes	no	REFER is sent towards inbound dial-peer
yes	yes	INVITE is sent towards refer-to dial-peer
no	no	INVITE is sent towards refer-to dial-peer
no	yes	INVITE is sent towards refer-to dial-peer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following:
 - **no supplementary-service sip refer** in global VoIP configuration mode.
 - **no supplementary-service sip refer** in dial-peer configuration mode.
4. **refer consume** in global VoIP configuration mode.
5. (Optional) **supplementary-service media-renegotiate** in global VoIP configuration mode.
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>Enter one of the following:</p> <ul style="list-style-type: none"> • no supplementary-service sip refer in global VoIP configuration mode. • no supplementary-service sip refer in dial-peer configuration mode. <p>Example:</p> <p>In global VoIP configuration mode:</p> <pre>Device(config)# voice service voip Device(conf-voi-serv)# no supplementary-service sip refer</pre> <p>Example:</p> <p>In dial-peer configuration mode:</p> <pre>Device(config)# dial-peer voice 22 voip Device(config-dial-peer)# no supplementary-service sip refer</pre>	<p>Configures REFER consumption. An INVITE is sent towards the Refer-to dial peer.</p>
Step 4	<p>refer consume in global VoIP configuration mode.</p> <p>Example:</p> <p>In dial-peer configuration mode:</p>	<p>Configures REFER consumption.</p>

	Command or Action	Purpose
	<pre>Device(config)# dial-peer voice 22 voip Device(config-dial-peer)# refer consume</pre>	
Step 5	<p>(Optional) supplementary-service media-renegotiate in global VoIP configuration mode.</p> <p>Example:</p> <p>In global VoIP configuration mode:</p> <pre>Device(config)# voice service voip Device(conf-voi-serv)# supplementary-service media-renegotiate</pre>	Enables end-to-end media renegotiation during the call transfer in REFER consumption mode.
Step 6	end	Exits to privileged EXEC mode.

Troubleshooting Tips

Use any of the following debug commands:

- **debug ccsip all**
- **debug voip ccapi inout**
- **debug sccp messages**
- **debug voip application supplementary-service**
- **debug voip application state**
- **debug voip application media negotiation**



CHAPTER 39

Cause Code Mapping

- [Overview, on page 385](#)
- [Cause Code Mapping, on page 386](#)
- [Configure Cause Code Mapping, on page 387](#)
- [Verify Cause Code Mapping, on page 388](#)

Overview

With the Cause Code Mapping feature, the NOTIFY message sent by Cisco Unified Border Element (CUBE) to a Customer Voice Portal (CVP) contains a proper reason for failure of call transfer based on the information received by CUBE from the caller instead of a 503 Service Unavailable message for all scenarios.

Feature Information

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 58: Feature Information for Cause Code Mapping

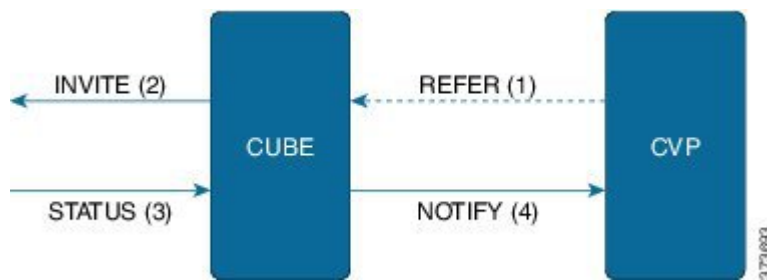
Feature Name	Releases	Feature Information
Cause Code Mapping	Cisco IOS XE 3.14S Cisco IOS 15.5(1)S3 Cisco IOS 15.5(2)S1 Cisco IOS 15.4(3)S4	With the Cause Code Mapping feature, the NOTIFY message sent by CUBE to a Customer Voice Portal (CVP) contains a proper reason for failure of call transfer based on the information received by CUBE from the caller. Following are the cause codes supported: <ul style="list-style-type: none">• 17—486 Busy Here• 19—503 Service Unavailable• 21—403 Forbidden• 31—480 Temporarily Unavailable• 102—504 Server Time-out

Cause Code Mapping

If CUBE is configured to consume REFERs that it receives, the following actions occur:

1. CUBE consumes the REFER that it receives from a Customer Voice Portal (CVP).
2. CUBE sends an INVITE (instead of a REFER) to the outbound leg (towards the caller).
3. CUBE receives a status from the caller.
4. CUBE sends a NOTIFY message to the CVP.

Figure 32: Refer Consume in CUBE



Previously, the NOTIFY message sent in step 4 included a 503 Service Unavailable message irrespective of the reason for failure of call transfer in step 3.

With the Cause Code Mapping feature, the NOTIFY message contains proper reason for failure of call transfer so that the CVP can take an appropriate action.

Table 59: Cause Code Mappings

Status Message received by CUBE (Step 3)	Cause Code	Notify message sent to CVP (Step 4)
486	17	486 Busy Here
480	31	480 Temporarily Unavailable
403	21	403 Forbidden
480	19	503 Service Unavailable
504	102	504 Server Time-out
404	1	404 Not Found
480	20	480 Temporarily Unavailable
484	28	484 Address Incomplete
502	27	502 Bad Gateway
503	38	503 Service Unavailable



Note Cause code mappings for cause code 19 and 21 require configurations mentioned in [Configure Cause Code Mapping, on page 387](#).



Note This mapping is only for the REFER consume scenario and not for REFER passthrough.

Configure Cause Code Mapping

SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. reason-header override
5. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	sip-ua Example: Device(config)# sip-ua	Enters the SIP user agent configuration mode.
Step 4	reason-header override Example: Device(config-sip-ua)# reason-header override	Configures the sending of a proper reason for failure of call transfer in the NOTIFY message so that the Customer Voice Portal (CVP) can take an appropriate action.
Step 5	end Example: Device(config-sip-ua)# end	Exits to privileged EXEC mode.

Verify Cause Code Mapping

SUMMARY STEPS

1. Enter the following:
 - **debug ccsip function**
 - **debug ccsip message**
 - **debug voip application state**
 - **debug voip application core**
 - **debug voip ccapi inout**

DETAILED STEPS

Enter the following:

- **debug ccsip function**
- **debug ccsip message**
- **debug voip application state**
- **debug voip application core**
- **debug voip ccapi inout**

Example:

486 Received by CUBE:

```
Received:
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP 9.40.3.231:5060;branch=z9hG4bK1C15625F7
From: <sip:2222@9.40.3.231>;tag=49B0964D-213C
To: <sip:3333@9.0.0.174>;tag=1
Call-ID: 7D7073E4-3F3B11E4-917BF9A9-A90B2232@9.40.3.231
CSeq: 101 INVITE
Allow-Events: telephone-event
Content-Length: 0
Reason: Q.850;cause=17
```

486 Busy here response sent in NOTIFY by CUBE

```
Sent:
NOTIFY sip:1111@9.0.0.174:9000 SIP/2.0
Via: SIP/2.0/UDP 9.40.3.231:5060;branch=z9hG4bK1C1571767
From: <sip:2222@9.40.3.231:5060>;tag=49B08E64-1374
To: <sip:1111@9.0.0.174>;tag=1
Call-ID: 1-25970@9.0.0.174
CSeq: 102 NOTIFY
Max-Forwards: 70
Date: Fri, 19 Sep 2014 13:55:46 GMT
User-Agent: Cisco-SIPGateway/IOS-15.5.20140712.124355.
Event: refer
Subscription-State: terminated;reason=noresource
Contact: <sip:2222@9.40.3.231:5060>
Content-Type: message/sipfrag
Content-Length: 25
```

SIP/2.0 486 Busy here



PART VII

Media Services

- [Codec Support and Restrictions, on page 393](#)
- [Codec Preference Lists, on page 399](#)
- [Payload Type Interoperability, on page 407](#)
- [Transcoding Configuration, on page 415](#)
- [Transrating Configuration, on page 419](#)
- [Call Progress Analysis , on page 421](#)
- [Fax Detection, on page 429](#)
- [Video Suppression, on page 441](#)
- [ICE-Lite Support, on page 445](#)
- [NAT Traversal using RTP Keepalive, on page 459](#)
- [Configure Report Generation, on page 467](#)



CHAPTER 40

Codec Support and Restrictions

- [Overview, on page 393](#)
- [OPUS Codec, on page 394](#)
- [ISAC Codec Support on CUBE, on page 396](#)
- [AAC-LD MP4A-LATM Codec Support, on page 396](#)

Overview

This chapter provides advanced information about the support of and restrictions for using certain codecs with CUBE. For basic information on how to configure codecs, refer to the [Overview, on page 63](#) section.

Feature Information

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 60: Feature Information for Codec Support

Feature Name	Releases	Feature Information
Opus Codec Transcoding	Cisco IOS XE Bengaluru 17.6.1a	Transcoding support was introduced for Opus codec.

Feature Name	Releases	Feature Information
Opus Codec Negotiation	Cisco IOS XE Amsterdam 17.3.1	<p>Opus audio codec support on CUBE was introduced.</p> <p>The following commands were introduced or modified as part of Opus codec feature:</p> <ul style="list-style-type: none"> • codec opus [profile tag] • codec profile tag profile • codec preference value codec-type [profile profile-tag] • rtp payload-type opus payload-type-number

OPUS Codec

The Opus interactive speech and audio codec is designed to handle a wide range of interactive audio applications. This includes Voice over IP, video conferencing, and in-game chat. The OPUS codec also supports live, distributed music performances. It scales from low bitrate narrowband speech at 6 kbps to very high-quality stereo music at 510 kbps. Opus uses both Linear Prediction (LP) and Modified Discrete Cosine Transform (MDCT) algorithms to achieve good compression of both speech and music.



Note Opus codec is only supported for SIP-SIP call scenarios. It is not supported for TDM-SIP or Analog-SIP flows.

Opus Codec Configuration

- You can configure Opus codec handling with the following dial peer and voice class codec commands:

- **codec opus** [**profile tag**] —The CLI command under **dial-peer** configuration mode is enhanced:

```
router(config)#dial-peer voice 3002 voip
router(config-dial-peer)#codec opus profile 2
```

- **codec profile tag profile** —The CLI command that is configured under global configuration mode is enhanced to configure **opus** as a supported codec:

```
router(config)#codec profile 2 opus
router(conf-codec-profile)#fmt "fmt:114 maxplaybackrate=16000;
sprop-maxcapture=16000; maxaveragebitrate=20000; stereo=1; sprop-stereo=0;
useinbandfec=0; usedtx=0; cbr=0"
router(conf-codec-profile)#exit
```

- **codec preference value codec-type** [**profile profile-tag**]—The CLI command that is configured under voice class configuration mode is enhanced to configure **opus** as a preferred codec on the dial-peer:

```
router(config)#voice class codec 80
router(config-class)#codec preference 1 opus profile 79
router(config-class)#exit
```

- **rtp payload-type [opus number]** —The CLI command that is configured under dial-peer configuration mode is enhanced to configure **opus** as a supported payload type:

```
router(config)#dial-peer voice 604 voip
router(config-dial-peer)#rtp payload-type opus 126
```

- The default payload-type for **opus** is set to 114.
- The default payload-type for **cisco-codec-aacld** is set to 112.
- The CLI command **show call active voice [brief | compact]** is modified to include details on Opus codec in the command output.
- The CLI command **show sip-ua calls** is modified to include details on Opus codec in the command output.
- Opus codec profile configuration is optional and can be used to define the initial offer in delayed offer to early offer call flows. Else, DSP-specific Opus parameters are used if the DSPFARM profile is configured with Opus codec.
- Transcoding between Opus and other codecs is available with PVD4 DSP cards from Cisco IOS XE Bengaluru 17.6.1a onwards. Calls that require Opus transcoding are dropped by earlier releases.
- Opus Codec is supported for both secure and nonsecure calls (RTP-to-RTP, SRTP-to-SRTP, SRTP-to-RTP, and RTP-to-SRTP).
- Opus supports several clock rates. Only the highest clock rate of 48000 is advertised in the SDP. The following is a sample configuration of SDP for Opus codec:


```
m=audio 16000 RTP/AVP 114          a=rtpmap:114 opus/48000/2
```
- Opus codec defines the optional media format (fmt) parameters in a call. CUBE passes through the optional **fmt** parameters from one side to the other if an Opus codec is configured on both sides of the call.
- Opus codec defines the following fmt parameters:
 - **maxaveragebitrate**
 - **maxplaybackrate**
 - **stereo**
 - **useinbandfec**
 - **usedtx**
 - **sprop-maxcapture**
 - **sprop-stereo**
 - **cbr**
- Dynamic payload interworking is enabled by default on CUBE. Configure **asymmetric payload [full]** if CUBE is not required to handle payload interworking. In this scenario, interworking is handled at the endpoints handling the media.

- For interworking scenarios that support Opus codec, SDP Offer-Answer by CUBE must include default fmtp parameters that are required by DSP. The Offer-Answer includes the DSP-specific default parameters only if DSPFARM is configured with Opus codec.

Example:

```
m=audio 4002 RTP/AVP 114
a=rtpmap:114 opus/48000/2
a=fmtp:114 maxaveragebitrate=32000
a=maxptime:20
```

Restrictions

- The Opus codec option is not available with the Extended Media Forking (XMF) API.
- CUBE doesn't support processing of multiple fmtp lines. If the received SDP has multiple fmtp lines, then only the first fmtp line is passed in the outbound INVITE.
- CUBE DSP doesn't support multiframe OPUS RTP packets for transcoding.

ISAC Codec Support on CUBE

The iSAC codec is an adaptive VoIP codec specially designed to deliver wideband sound quality in both low- and high-bit rate applications. The iSAC codec automatically adjusts the bit-rate for the best quality or a fixed bit rate can be used if the network characteristics are known. This codec is designed for wideband VoIP communications. The iSAC codec offers better quality with reduced bandwidth for sideband applications.

Restrictions

Low complexity is not supported for the iSAC codec.

AAC-LD MP4A-LATM Codec Support

As part of this feature, CUBE supports the following:

- Accept and send MP4A-LATM codec and corresponding FMTP profiles
- Configure MP4A-LATM under dial-peer or under voice-class codec as preferred codec
- Pass across real-time transport protocol (RTP) media for MP4A-LATM codec without any interworking
- Offer pre-configured FMTP profile for MP4A-LATM for DO-EO (Delayed-Offer to Early-Offer) calls
- Offer more than one FMTP profile (each with different payload type number) as mentioned by the offering endpoint, so that the answering endpoint can choose the best option.
- Offer only one instance of MP4A-LATM if media forking is applicable. The offered instance is the first one received in the offer.

- Calculate bandwidth for MP4A-LATM on the basis of either “b=TIAS” attribute or “bitrate” parameter in the FMTP attribute. If none of them are present in the session description protocol (SDP), the default maximum bandwidth, that is, 128 Kbps will be used for calculation.
- The following CUBE features are supported with the MP4A-LATM codec:
 - Basic call (audio and video) flow-around and flow-through (FA and FT).
 - Voice Class Codec support in CUBE with codec filtering
 - SRTP and SRTCP passthrough for SIP-to-SIP calls
 - Supplementary services
 - RSVP
 - Dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls
 - Media Anti-Trombone with SIP signaling control on CUBE
 - Support for SIP UPDATE message per RFC 3311
 - RTP Media Loopback
 - Media forking for IP based calls using Zephyr recording server
 - CUBE Mid-call Re-INVITE consumption
 - Signaling forking (Fastweb multile SIP Early Dialog Support, FA and FT)
 - Maximum bandwidth-based CAC
 - Media Policing
 - Box-to-Box High Availability (B2B HA)
 - Inbox High Availability (Inbox HA)

Restrictions for AAC-LD MP4A-LATM Codec Support

CUBE does not support the following:

- Codec transcoding between MP4A-LATM and other codecs
- Dual-tone Multifrequency (DTMF) interworking with MP4A-LATM codec
- Non-SIP-SIP, that is, SIP to other service provider interface (SPI) interworking with MP4A-LATM codec



CHAPTER 41

Codec Preference Lists

- [Overview, on page 399](#)
- [Codecs Configured Using Preference Lists, on page 400](#)
- [Restrictions, on page 400](#)
- [Configure Audio Codecs Using a Codec Voice Class and Preference Lists, on page 401](#)
- [Disable Codec Filtering, on page 402](#)
- [Troubleshoot Negotiation of an Audio Codec from a List of Codecs, on page 403](#)
- [Verify Negotiation of an Audio Codec from a List of Codecs, on page 404](#)

Overview

This chapter describes how to negotiate an audio codec from a list of codec associated with a preference. This chapter also describes how to disable codec filtering by configuring Cisco Unified Border Element (CUBE) to send an outgoing offer with all configured audio codecs in the list assuming that the dspfarm supports all these codecs.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 61: Feature Information for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Feature Name	Releases	Feature Information
Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the CUBE	Baseline Functionality	The following command was introduced or modified: voice-class codec (dial-peer)

Codecs Configured Using Preference Lists

The list of codecs supported in a SIP-to-SIP call can be configured with a Codec Preference List on each SIP call leg with following properties:

- Incoming and outgoing dial-peers can be configured with different preference lists.
- Midcall codec changes for supplementary services are supported with preference lists. Transcoder resources are dynamically inserted or deleted when there is a codec or RTP-NTE to in-band DTMF interworking required.
- Reinvite-based supplementary services that are invoked from the Cisco Unified Communications Manager (CUCM), like call hold, call resume, Music On Hold (MOH), call transfer, and call forward are supported with preference lists.
- T.38 fax and fax passthrough switchover with preference lists are supported.
- Reinvite-based call hold and call resume for the Secure Real-Time Transfer protocol (SRTP) and Real-Time Transport Protocol (RTP) interworking on CUBE is supported with preference lists.
- High availability is supported for calls that use codecs with preference lists. But calls requiring the transcoder to be invoked are not checkpointed. During midcall renegotiation, if the call releases the transcoder, then the call is checkpointed.

Restrictions

For All Calls (SIP-to-SIP calls)

- Video codecs are not supported with preference lists.
- Multiple audio streams are not supported.
- Codec re-packetization feature is not supported when preference lists are configured.



Note

Codec preference in the voice class codec on the outgoing call leg is not followed when the same codecs are available in the respective incoming invite with SDP with different codec preference. Cube prioritizes and follows the incoming invite with SDP codec preference when compared to the voice class codec preference on the outgoing dial-peer leg.

Configure Audio Codecs Using a Codec Voice Class and Preference Lists

Preferences can be used to determine which codecs will be selected over others.

A codec voice class is a construct within which a codec preference order can be defined. A codec voice class can then be applied to a dial peer, which then follows the preference order defined in the codec voice class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class codec tag**
4. Do the following for each audio codec you want to configure in the voice class:
 - **codec preference value codec-type**[profile profile-tag]
 - **codec preference value codec-type**[bytes payload-size fixed-bytes]
 - **codec preference value isac** [mode {adaptive | independent} [bit-rate value framesize { 30 | 60 } [fixed]]
 - **codec preference value ilbc** [mode frame-size [bytes payload-size]]
 - **codec preference value mp4-latm** [profile tag]
5. **exit**
6. **dial-peer voice number voip**
7. **voice-class codec tag**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device> configure terminal	Enters global configuration mode.
Step 3	voice class codec tag Example: Device(config)# voice class codec 10	Enters voice-class configuration mode for the specified codec voice class.
Step 4	Do the following for each audio codec you want to configure in the voice class: <ul style="list-style-type: none"> • codec preference value codec-type[profile profile-tag] 	Configure a codec within the voice class and specifies a preference for the codec. This becomes part of a preference list

	Command or Action	Purpose
	<ul style="list-style-type: none"> • codec preference <i>value codec-type</i>[bytes <i>payload-size</i> <i>fixed-bytes</i>] • codec preference <i>value isac</i> [mode {adaptive independent} [bit-rate <i>value</i> framesize { 30 60 } [fixed]] • codec preference <i>value ilbc</i> [mode <i>frame-size</i> [bytes <i>payload-size</i>]] • codec preference <i>value mp4-latm</i> [profile <i>tag</i>] 	
Step 5	exit Example: Device(config-class)# exit	Exits the current mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 6	dial-peer voice <i>number voip</i> Example: Device(config)# dial-peer voice 1 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 7	voice-class codec <i>tag</i> Example: Device(config-dial-peer)# voice-class codec 10	Applies the previously configured voice class and associated codecs to a dial peer.
Step 8	end Example: Device(config-dial-peer)# end	Returns to privileged EXEC mode.

Disable Codec Filtering

CUBE is configured to filter common codecs for the subsets, by default. The filtered codecs are sent in the outgoing offer. You can configure the CUBE to offer all the codecs configured on an outbound leg instead of offering only the filtered codecs.



Note This configuration is applicable only for early offer calls from the CUBE. For delayed offer calls, by default all codecs are offered irrespective of this configuration.

Perform this task to disable codec filtering and allow all the codecs configured on an outbound leg.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag voip*
4. **voice-class codec** *tag offer-all*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# dial-peer voice 10 voip	Enters dial peer voice configuration mode.
Step 4	voice-class codec tag offer-all Example: Device(config-dial-peer)# voice-class codec 10 offer-all	Adds all the configured voice class codec to the outgoing offer from the CUBE.
Step 5	end Example: Device(config-dial-peer)# end	Exits the dial peer voice configuration mode.

Troubleshoot Negotiation of an Audio Codec from a List of Codecs

Use the following commands to debug any errors that you may encounter when you configure the Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the CUBE feature:

- **debug ccsip all**
- **debug voip ccapi input**
- **debug voip rtp session**

For DSP-related debugs, use the following commands:

- **debug voip dsmp all**
- **debug voip dsmp rtp both payload all**
- **debug voip ipipgw**

Verify Negotiation of an Audio Codec from a List of Codecs

Perform this task to display information to verify Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element configuration. These **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call active voice brief**
3. **show voip rtp connections**
4. **show dspfarm dsp active**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Step 2 show call active voice brief

Displays a truncated version of call information for voice calls in progress.

Example:

```
Device# show call active voice brief
<ID>: <CallID> <start>ms.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
  IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
  media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
  long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
  last <buf event time>s dur:<Min>/<Max>s
  FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
  ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
  Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
  speeds(bps): local <rx>/<tx> remote <rx>/<tx>
  Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
  bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
  rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
  Telephony call-legs: 0
  SIP call-legs: 2
  H323 call-legs: 0
  Call agent controlled call-legs: 0
  SCCP call-legs: 2
  Multicast call-legs: 0
  Total call-legs: 4
  1243 : 11 971490ms.1 +-1 pid:1 Answer 1230000 connecting
  dur 00:00:00 tx:415/66400 rx:17/2561
  IP 192.0.2.1:19304 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
  media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
```

```

long duration call detected:n long duration call duration:n/a timestamp:n/a
1243 : 12 971500ms.1 +-1 pid:2 Originate 3210000 connected
dur 00:00:00 tx:5/10 rx:4/8
IP 9.44.26.4:16512 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
0 : 13 971560ms.1 +0 pid:0 Originate connecting
dur 00:00:08 tx:415/66400 rx:17/2561
IP 192.0.2.2:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
0 : 15 971570ms.1 +0 pid:0 Originate connecting
dur 00:00:08 tx:5/10 rx:3/6
IP 192.0.2.3:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4

```

Step 3 show voip rtp connections

Displays Real-Time Transport Protocol (RTP) connections.

Example:

```

Device# show voip rtp connections
VoIP RTP active connections :
No. CallId      dstCallId LocalRTP RmtRTP      LocalIP      RemoteIP
1      11      12      16662      19304      192.0.2.1
192.0.2.2
2      12      11      17404      16512      192.0.2.2
192.0.2.3
3      13      14      18422      2000      192.0.2.4
9.44.26.3
4      15      14      16576      2000      192.0.2.6
192.0.2.5
Found 4 active RTP connections

```

Step 4 show dspfarm dsp active

Displays active DSP information about the DSP farm service.

Example:

```

Device# show dspfarm dsp active
SLOT DSP VERSION STATUS CHNL USE TYPE RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED
0 1 27.0.201 UP 1 USED xcode 1 0x9 5 8
0 1 27.0.201 UP 1 USED xcode 1 0x8 2558 17
Total number of DSPFARM DSP channel(s) 1

```




CHAPTER 42

Payload Type Interoperability

-
- [Overview, on page 407](#)
- [Restrictions , on page 408](#)
- [Symmetric and Asymmetric Calls, on page 408](#)
- [High Availability Checkpointing Support for Asymmetric Payload, on page 409](#)
- [Configure Dynamic Payload Type Passthrough for DTMF and Codec Packets for SIP-to-SIP Calls, on page 409](#)
- [Configuration Examples for Assymmetric Payload Interworking, on page 413](#)

Overview

The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for dual tone multifrequency (DTMF) and codec packets for Session Initiation Protocol (SIP) to SIP calls.

Based on this feature, the Cisco Unified Border Element (CUBE) interworks between different dynamic payload type values across the call legs for the same codec. Also, CUBE supports any payload type value for audio, video, named signaling events (NSEs), and named telephone events (NTEs) in the dynamic payload type range 96 to 127.

Feature Information

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 62: Feature Information for Dynamic Payload Interworking for DTMF and Codec Packets Support

Feature Name	Releases	Feature Information
Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls	Baseline Functionality	<p>The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls.</p> <p>The following commands were introduced or modified: asymmetric payload and voice-class sip asymmetric payload.</p>

Restrictions

The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature is not supported for the following:

- Transcoded calls in releases prior to Cisco IOS XE Bengaluru 17.6.1a.
- Secure Real-Time Protocol (SRTP) pass-through calls.
- Flow-around calls.
- Asymmetric payload types are not supported on early-offer (EO) call legs in a delayed-offer to early-offer (DO-EO) scenario.
- Cisco fax relay.
- Multiple m lines with the same dynamic payload types, where m is:

$m = \text{audio } \langle \text{media-port1} \rangle \text{ RTP/AVP XXX } m = \text{video } \langle \text{media-port2} \rangle \text{ RTP/AVP XXX}$

Symmetric and Asymmetric Calls

CUBE supports dynamic payload type negotiation and interworking for all symmetric and asymmetric payload type combinations. A call leg on CUBE is considered as symmetric or asymmetric based on the payload type value exchanged during the offer and answer with the endpoint:

- A symmetric endpoint accepts and sends the same payload type.
- An asymmetric endpoint can accept and send different payload types.

The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature is enabled by default for a symmetric call. An offer is sent with a payload type based on the dial-peer configuration. The answer is sent with the same payload type as was received in the incoming offer. When the payload type values negotiated during the signaling are different, the CUBE changes the Real-Time Transport Protocol (RTP) payload value in the VoIP to RTP media path.

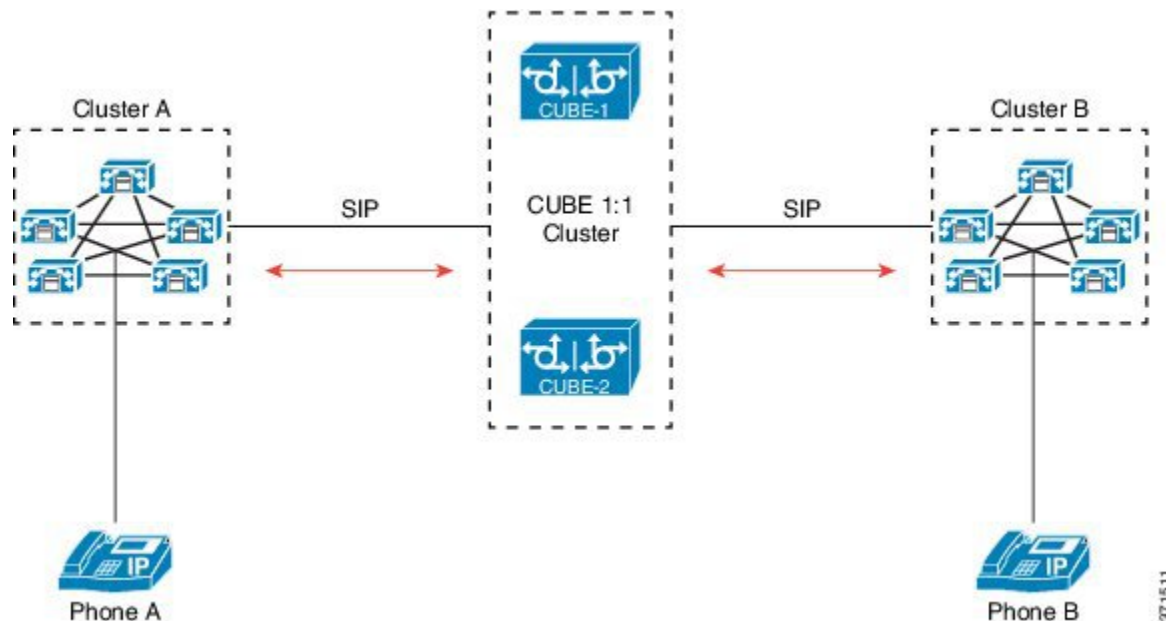
To support asymmetric call legs, you must enable The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature. The dynamic payload type value is passed across the call legs,

and the RTP payload type interworking is not required. The RTP payload type handling is dependent on the endpoint receiving them.

High Availability Checkpointing Support for Asymmetric Payload

High availability for a call involving asymmetric payloads is supported. In case of fail-over from active to stand-by, the asymmetric payload interworking will be continued as new active CUBE passes across the payload type values according to the negotiation and call establishment.

Figure 33: Sample High-Availability Topology



Configure Dynamic Payload Type Passthrough for DTMF and Codec Packets for SIP-to-SIP Calls

Configure Dynamic Payload Type Passthrough at the Global Level

Perform this task to configure the pass through of DTMF or codec payload to the other call leg (instead of performing dynamic payload type interworking) feature at the global level.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `asymmetric payload {dtmf | dynamic-codecs | full | system}`

6. end

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	voice service voip Example: Device(config)# voice service voip	Enters voice service configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# sip	Enters voice service SIP configuration mode.
Step 5	asymmetric payload {dtmf dynamic-codecs full system} Example: Device(conf-serv-sip)# asymmetric payload full	Configures global SIP asymmetric payload support. Note The dtmf and dynamic-codecs keywords are internally mapped to the full keyword to provide asymmetric payload type support for audio and video codecs, DTMF, and NSEs.
Step 6	end Example: Device(conf-serv-sip)# end	Exits voice service SIP configuration mode and enters privileged EXEC mode.

Configure Dynamic Payload Type Passthrough for a Dial Peer

Perform this task to configure the pass through of DTMF or codec payload to the other call leg (instead of performing dynamic payload type interworking) feature at the dial-peer level.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip asymmetric payload {dtmf | dynamic-codecs | full | system}

5. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# dial-peer voice 77 voip	Enters dial peer voice configuration mode.
Step 4	voice-class sip asymmetric payload {dtmf dynamic-codecs full system} Example: Device(config-dial-peer)# voice-class sip asymmetric payload full	Configures the dynamic SIP asymmetric payload support. Note The dtmf and dynamic-codecs keywords are internally mapped to the full keyword to provide asymmetric payload type support for audio and video codecs, DTMF, and NSEs.
Step 5	end Example: Device(config-dial-peer)# end	(Optional) Exits dial peer voice configuration mode and enters privileged EXEC mode.

Verify Dynamic Payload Interworking for DTMF and Codec Packets Support

This task shows how to display information to verify Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls configuration feature. These **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. enable
2. show call active voice compact
3. show call active voice

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show call active voice compact Example: Device# show call active voice compact	(Optional) Displays a compact version of call information.
Step 3	show call active voice Example: Device# show call active voice	(Optional) Displays call information for voice calls in progress.

Tips to Troubleshoot

Use the following commands to debug errors while configuring the Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature:

- **debug ccsip all**
- **debug voip ccapi inout**
- **debug voip rtp**

Use the following debug commands to troubleshoot HA Checkpointing for Asymmetric Payload:

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

Use the following **show** commands to troubleshoot HA Checkpointing for Asymmetric Payload:

- **show redundancy state**
- **show redundancy inter-device**
- **show standby brief**
- **show voice high-availability summary**
- **show voip rtp stats**

- **show voip rtp high-availability stats**
- **show voip rtp connection detail**
- **show call active voice brief**
- **show call active voice [summary]**
- **show call active video brief**
- **show call active video [summary]**
- **show align**
- **show memory debug leak**

Configuration Examples for Assymmetric Payload Interworking

Example: Asymmetric Payload Interworking—Passthrough Configuration

```
!  
voice service voip  
  allow-connections sip to sip  
sip  
  rel1xx disable  
  asymmetric payload full  
  midcall-signaling passthru  
!  
dial-peer voice 1 voip  
  voice-class sip asymmetric payload full  
  session protocol sipv2  
  rtp payload-type cisco-codec-fax-ind 110  
  rtp payload-type cisco-codec-video-h264 112  
  session target ipv4:9.13.8.23  
!
```

In the above example, it is assumed that 110 and 112 are not used for any other payload.

Example: Asymmetric Payload Interworking—Interworking Configuration

```
!  
voice service voip  
  allow-connections sip to sip  
!  
dial-peer voice 1 voip  
  session protocol sipv2  
  rtp payload-type cisco-codec-fax-ind 110  
  rtp payload-type cisco-codec-video-h264 112  
  session target ipv4:9.13.8.23  
!
```

In the above example, it is assumed that 110 and 112 are not used for any other payload.



CHAPTER 43

Transcoding Configuration

- [Overview, on page 415](#)
- [Configure LTI-Based Transcoding, on page 416](#)
- [Configuration Examples for LTI Based Transcoding, on page 417](#)
- [Verify Configuration, on page 418](#)
- [VoIP Trace Logging, on page 418](#)

Overview

Transcoding is a process that converts a media stream encoded with one algorithm to another using Digital Signal Processors (DSPs). For example, a media stream encoded using OPUS may be decoded and re-encoded (transcoded) using G.711.



Note In high availability configurations, checkpoint for transcoded calls require both the standby system and its DSPs to be ready when a call begins. Calls that are set up before the standby resources are ready will not be maintained on failover.

LTI based Transcoding

- Internal API is used to access Digital Signal Processor (DSP) resources for transcoding.
- Transcoding resources (DSPFARM) and CUBE must be on the same platform.
- Only DSPFARM profile configuration is required. Skinny Client Control Protocol (SCCP) configuration is not required.
- No TCP socket is opened and no registration is used.
- DSPFARM profile is associated to application type CUBE.

```
Device(config)# dspfarm profile 1 transcode
Device(config-dspfarm-profile)# associate application CUBE
```

- DSPs are not used for encryption with IOS XE. As all media is encrypted or decrypted as it leaves or enters the platform, transcoding may be used for any combination of RTP-RTP, RTP-SRTP, or SRTP-SRTP calls.



Note The following support LTI-based transcoding:

- Cisco Aggregated Services Routers 1000 Series (ASR 1K)
- Cisco 4000 Series-Integrated Services Routers (ISR G3)
- Cisco 8200 Catalyst Edge Series
- Cisco 8300 Catalyst Edge Series

Limitations

- Video transcoding is not supported. This document only refers to transcoding for CUBE B2BUA calls. Refer to [System Configuration Guide for Cisco Unified Communications Manager](#) for UCM MTP details.
- SCCP-based transcoding is not supported with IOS XE releases.
- Transcoding cannot be used for SRTP-Passthrough calls or when pass-thru content SDP is enabled.

Configure LTI-Based Transcoding



Note • Opus transcoding is only supported by PVDM4 modules.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *voice-interface-slot-number*
4. **dsp services dspfarm**
5. **exit**
6. **dspfarm profile** *profile-identifier* **transcode**
7. **codec** *codec*
8. **maximum sessions** *sessions*
9. **associate application** **CUBE**
10. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device> configure terminal	Enters global configuration mode.
Step 3	voice-card voice-interface-slot-number Example: Device(config)# voice-card 0/2	Configures a voice card and enters voice-card configuration mode.
Step 4	dsp services dspfarm	Enable voice-only DSP services on the Voice Card.
Step 5	exit	Exits the voice-card configuration mode.
Step 6	dspfarm profile profile-identifier transcode Example: Device(config)# dspfarm profile 2 transcode	Enters a DSP farm profile configuration mode and defines a profile for DSP farm services. <ul style="list-style-type: none"> • <i>profile-identifier</i>- Number that uniquely identifies a profile. Range: 1–65535. • transcode- Enables profile for transcoding.
Step 7	codec codec Example: Device(config-dspfarm-profile)# codec opus	Add a list of codecs that you wish to transcode.
Step 8	maximum sessions sessions	Configures maximum number of transcoding sessions.
Step 9	associate application CUBE	Configures an application to the profile for LTI-based transcoding.
Step 10	no shutdown Example: Device (config-dsp-farm-profile) # no shutdown	Allocates DSP resources and associates with the application.

Configuration Examples for LTI Based Transcoding

Example: LTI-based Transcoding

```
! Enabling dspfarm services under voice-card
Device(config)# voice-card 0/2
Device(config-voicecard)# dsp services dspfarm
Device(config-voicecard)# exit
! Configuring dspfarm profile
Device(config)# dspfarm profile 2 transcode
Device(config-dspfarm-profile)# codec g729abr8
Device(config-dspfarm-profile)# codec g729ar8
Device(config-dspfarm-profile)# codec g711alaw
Device(config-dspfarm-profile)# codec g711ulaw
Device(config-dspfarm-profile)# codec g722-64
```

```

Device(config-dspfarm-profile)# codec opus
Device(config-dspfarm-profile)# maximum sessions 10
Device(config-dspfarm-profile)# associate application CUBE
Device(config-dspfarm-profile)# no shutdown

```

Verify Configuration

```

Device#show dspfarm profile
Profile ID = 2, Service = TRANSCODING, Resource ID = 2
Profile Service Mode : Non Secure
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : CUBE   Status : ASSOCIATED
Resource Provider : FLEX_DSPRM   Status : UP
Total Number of Resources Configured : 10
Total Number of Resources Available : 10
Total Number of Resources Out of Service : 0
Total Number of Resources Active : 0
Codec Configuration: num_of_codecs:6
Codec : opus, Maximum Packetization Period : 120
Codec : g722-64, Maximum Packetization Period : 30
Codec : g711ulaw, Maximum Packetization Period : 30
Codec : g711alaw, Maximum Packetization Period : 30
Codec : g729ar8, Maximum Packetization Period : 60
Codec : g729abr8, Maximum Packetization Period : 60
Device#

```

VoIP Trace Logging

VoIP Trace is used for event logging and debugging of VoIP parameters. Using the VoIP Trace framework, the following information is recorded for transcoded calls at CUBE:

- Reservation
- Association
- Disassociation

The following is a sample output for VoIP Trace logging specific to transcoded calls at CUBE:

```

Apr 16 11:32:42.910: //63/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_reserve (0)
Apr 16 11:32:42.926: //63/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_associate (0)
Apr 16 11:32:42.942: //63/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_disassociate (0)
Apr 16 11:32:42.946: //62/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_disassociate (-1)
Apr 16 11:32:42.948: //63/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_disassociate_success
(0)
Apr 16 11:32:43.910: //66/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_reserve (-1)
Apr 16 11:32:44.926: //66/32191ED78080/CUBE_VT/SIP/API: ccsip_xcoder_associate (-1)

```



CHAPTER 44

Transrating Configuration

- [Transrating, on page 419](#)
- [Voice Packetization, on page 419](#)
- [Configure Transrating for a Codec, on page 420](#)

Transrating

Transrating is a process of configuring a different packetization for a voice codec. For example, transrating G.729 20ms to G.729 30ms.

Voice Packetization

After the voice wavelength is digitized, the DSP collects the digitized data for an amount of time until there is enough data to fill the payload of a single packet.

With G.711, either 20 ms or 30 ms worth of voice is transmitted in a single packet. 20 ms worth of voice corresponds to 160 samples per packet. With 20 ms worth of voice per packet, 50 packets are created per second: $1 \text{ sec} / 20 \text{ ms} = 50$.

The packetization rate has a direct effect on the total amount of bandwidth needed. More packets require more headers, and each header adds 40 bytes to the packet.

Codecs such as G.729 also compress the digitized output. G.729 creates a codeword for every 10 ms of voice. This “codeword” is a predefined representation of a 10-ms sample of human voice. Two codewords are contained in each packet at 50 packets per second or three codewords at 33.3 packets per second. Because the codewords need fewer bits, the overall bandwidth required is reduced.

Table 63: Packetization for different Codecs

Supported Codecs	Packetization (ms)
G.711 a-law 64 Kbps	10, 20, 30
G.711 law 64 Kbps	10, 20, 30
G.723 5.3/6/3 Kbps	30, 60
G.729, G.729A, G.729B, G.729AB 8 Kbps	10, 20, 30, 40, 50, 60

Supported Codecs	Packetization (ms)
G.722—64 Kbps	10, 20, 30

Configure Transrating for a Codec

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. **codec *codec-name* bytes *voice-payload-size* [fixed-bytes]**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device> configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>number</i> voip Example: Device(config)# dial-peer voice 1 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 4	codec <i>codec-name</i> bytes <i>voice-payload-size</i> [fixed-bytes] Example: Device(config-dial-peer)# codec g729r8 bytes 30 fixed-byte	Configures a different packetizations for a voice codec.
Step 5	end Example: Device(config-dial-peer)# end	Exits to privileged EXEC mode.



CHAPTER 45

Call Progress Analysis

- [Call Progress Analysis Over IP-to-IP Media Session, on page 421](#)
- [Feature Information for Call Progress Analysis Over IP-IP Media Session, on page 422](#)
- [Restrictions for Call Progress Analysis Over IP-to-IP Media Session, on page 423](#)
- [Configure Call Progress Analysis Over IP-to-IP Media Session, on page 424](#)

Call Progress Analysis Over IP-to-IP Media Session

The Call Progress Analysis Over IP-IP Media Session feature enables the detection of automated answering systems and live human voices on outbound calls and communicates the detected information to the external application. Typically, call progress analysis (CPA) is extensively used in contact center deployments in conjunction with the outbound Session Initiation Protocol (SIP) dialer, where CPA is enabled on the Cisco Unified Border Element (CUBE), and digital signal processors (DSP) perform the CPA functionality.

Call Progress Analysis

Call progress analysis (CPA) is a DSP algorithm that analyzes the Real-Time Transport Protocol (RTP) voice stream to look for special information tones (SIT), fax or modem tones, human speech, and answering machine tones. CPA also passes the voice information to Cisco IOS or CUBE.

CPA is initiated on receiving a new SIP INVITE with x-cisco-cpa content. While a call is in progress, the DSP or the Xcoder analyzes the incoming voice or media stream. The DSP identifies the type of voice stream based on statistical voice patterns or specific tone frequencies and provides the information to the CUBE. The CUBE notifies the dialer with a SIP UPDATE with x-cisco-cpa content along with the detected event. Based on the report, the caller (dialer) can decide to either transfer the call or terminate the call.

To use the CPA functionality, you must enable CPA and configure CPA timing and threshold parameters.

Table 64: X-cisco-cpa content meaning

SIP Message	Direction of Message	Meaning
18x or 200	Cisco IOS to dialer	CUBE informs the dialer if CPA is enabled for a call or not.
New INVITE	Dialer to Cisco IOS	Dialer requests Cisco IOS or the CUBE to activate the CPA algorithm for this session.

SIP Message	Direction of Message	Meaning
UPDATE	Cisco IOS to dialer	Cisco IOS or the CUBE notifies the dialer about the detected event.

CPA Events

Table 65: CPA Event Detection List

CPA Event	Definition
Asm	Answer machine
AsmT	Answer machine terminate tone
CpaS	Start of the Call Progress Analysis
FT	Fax/Modem tone
LS	Live human speech
LV	Low volume or dead air call
SitIC	Special information tone IC -- Intercept -- Vacant number or Automatic Identification System (AIS)
SitNC	SIT tone NC—No Circuit (NC), Emergency, or Trunk Blockage
SitVC	SIT tone VC—Vacant Code
SitRO	SIT tone RO—Reorder Announcement
SitMT	Miscellaneous SIT Tone

Feature Information for Call Progress Analysis Over IP-IP Media Session

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 66: Feature Information for Call Progress Analysis Over IP-IP Media Session

Feature Name	Releases	Feature Information
Call Progress Analysis Over IP-to-IP Media Session	15.3(2)T	The Call Progress Analysis Over IP-to-IP Media Session feature enables detection of automated answering systems and live human voices on outbound calls and communicates the detected information to an external application. The following command was introduced: call-progress-analysis.
Call Progress Analysis Over IP-to-IP Media Session	Cisco IOS XE Release 3.9S	The Call Progress Analysis Over IP-to-IP Media Session feature enables detection of automated answering systems and live human voices on outbound calls and communicates the detected information to an external application. The following command was introduced: call-progress-analysis.
Support for additional call flows	15.5(2)T Cisco IOS XE Release 3.15S	Call Progress Analysis feature is enhanced to support the following call-flows: <ul style="list-style-type: none"> • 180 SIP response received without SDP • Direct call connect (without 18x from Service Provider) • Multiple 18x response to INVITE • Early dialog UPDATE • Dialer-CUBE CPA call record

Restrictions for Call Progress Analysis Over IP-to-IP Media Session

- Only SIP-to-SIP Early Offer (EO-to-EO) call flows are supported.
- Session Description Protocol (SDP) passthrough and flow-around media calls are not supported.
- Only the G711 flavor of codec is supported.
- High Availability (HA) is not supported.
- Skinny Client Control Protocol (SCCP)-based digital signal processor (DSP) farm is not supported.
- CPA cannot not be detected if Dialer uses Inband as DTMF relay mechanism, that is, Inband to RTP-NTE DTMF inter-working is not supported with CPA.

- CPA call record is not supported for "180 without SDP" and "Direct Call Connect (without 18x)" call flows from Service Provider.
- With VCC codec configured on the dial-peer, the list of codecs in the VCC should match with the list of codec provisioned in DSP transcoder profile when CPA is enabled.

Configure Call Progress Analysis Over IP-to-IP Media Session

Enable CPA and Setting the CPA Parameters

Perform the following task to enable CPA and set the CPA timing and threshold parameters:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dspfarm profile profile-identifier transcode`
4. `call-progress-analysis`
5. `exit`
6. `voice service voip`
7. `cpa timing live-person max-duration`
8. `cpa timing term-tone max-duration`
9. `cpa threshold active-signal signal-threshold`
10. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dspfarm profile <i>profile-identifier</i> transcode Example: Device(config)# dspfarm profile 15 transcode	Enters DSP farm profile configuration mode, defines a profile for DSP farm services, and enables the profile for transcoding.
Step 4	call-progress-analysis Example:	Enables call progress analysis (CPA) on CUBE. <ul style="list-style-type: none"> • You must configure this command to activate the CPA feature and set CPA parameters.

	Command or Action	Purpose
	Device(config-dspfarm-profile)# call-progress-analysis	
Step 5	exit Example: Device(config-dspfarm-profile)# exit	Exits DSP farm profile configuration mode and enters global configuration mode.
Step 6	voice service voip Example: Device(config)# voice service voip	Enters voice service configuration mode.
Step 7	cpa timing live-person max-duration Example: Device(conf-voi-serv)# cpa timing live-person 2501	(Optional) Sets the maximum waiting time (in milliseconds) that the CPA algorithm uses to determine if a call is answered by a live human.
Step 8	cpa timing term-tone max-duration Example: Device(conf-voi-serv)# cpa timing term-tone 15500	(Optional) Sets the maximum waiting time (in milliseconds) that the CPA algorithm uses to wait for the answering machine termination tone after the answering machine is detected.
Step 9	cpa threshold active-signal signal-threshold Example: Device(conf-voi-serv)# cpa threshold active-signal 18db	(Optional) Sets the threshold (in decibels) of an active signal that is related to the measured noise floor level. <ul style="list-style-type: none"> • If a signal threshold configured by this command is greater than the measured noise floor level, then the signal is considered as active. The active signal thresholds that you can configure are 9, 12, 15, 18, and 21 decibels.
Step 10	end Example: Device(conf-voi-serv)# end	Exits voice service configuration mode and returns to privileged EXEC mode.

Example: Enabling CPA and Setting the CPA Parameters

The following example shows how to enable CPA and set a few timing and threshold parameters. Depending on your requirements, you can configure more timing and threshold parameters.

```
Device> enable
Device# configure terminal
Device(config)# dspfarm profile 15 transcode
Device(config-dspfarm-profile)# call-progress-analysis
```

```

Device(config-dspfarm-profile)# exit
Device(config)# voice service voip
Device(conf-voi-serv)# cpa timing live-person 2501
Device(conf-voi-serv)# cpa timing term-tone 15500
Device(conf-voi-serv)# cpa threshold active-signal 18db
Device(conf-voi-serv)# end

```

Verify the Call Progress Analysis Over IP-to-IP Media Session

Perform this task to verify that call progress analysis has been configured for a digital signal processor (DSP) farm profile.

SUMMARY STEPS

1. **enable**
2. **show dspfarm profile** *profile-identifier*

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show dspfarm profile *profile-identifier*

Displays the configured DSP farm profile information for a selected Cisco Call Manager group. In the following sample output, the Call Progress Analysis field shows that CPA is enabled.

Example:

```

Device# show dspfarm profile 3

Profile ID = 3, Service =Universal TRANSCODING, Resource ID = 3
Profile Description :
Profile Service Mode : Non Secure
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : CUBE Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Number of Resource Configured : 4
Number of Resources Out of Service : 0
Number of Resources Active : 0
Codec Configuration: num_of_codecs:4
Codec : g711ulaw, Maximum Packetization Period : 30
Codec : g711alaw, Maximum Packetization Period : 30
Codec : g729ar8, Maximum Packetization Period : 60
Codec : g729abr8, Maximum Packetization Period : 60
Noise Reduction : ENABLED
Call Progress Analysis : ENABLED

```

Tips to Troubleshoot

Use the following commands to troubleshoot the call progress analysis for SIP-to-SIP calls:

- **debug ccsip all**
- **debug voip ccapi inout**
- **debug voip hpi all**
- **debug voip ipipgw**
- **debug voip media resource provisioning all**



CHAPTER 46

Fax Detection

- [Overview, on page 429](#)
- [Restrictions for Fax Detection for SIP Call and Transfer on Cisco IOS XE, on page 430](#)
- [Information About Fax Detection for SIP Call and Transfer, on page 430](#)
- [Fax Detection with Cisco IOS XE High Availability, on page 433](#)
- [Fax Detection Configuration for SIP Calls, on page 433](#)
- [Configuration Examples for Fax Detection for SIP Calls, on page 439](#)

Overview

The fax detection feature detects whether an inbound call is from a fax machine. If the inbound call is from a fax machine, the call is rerouted appropriately.

Feature Information for Fax Detection for SIP Call and Transfer

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 67: Feature Information for Fax Detection for SIP Call and Transfer

Feature Name	Releases	Feature Information
Fax Detection for SIP Call and Transfer	Cisco IOS 15.4(2)T	Fax detection is the capability to detect automatically whether an incoming call is voice or fax. For calls coming from an IP trunk to CUBE, the Fax Detection for SIP Call and Transfer feature is used to detect CNG tones (calling tones) so that the fax server can handle the actual fax transmission or redirect the fax call to a configured fax number. The following commands were introduced: cng-fax-detect and detect-fax mode .
Fax Detection for SIP Call and Transfer on Cisco IOS XE Platforms	Cisco IOS XE Amsterdam 17.2.1r	Support was introduced for SIP call and transfer for IP-to-IP calls on Cisco IOS XE platforms for Cisco Unified Border Element.

Restrictions for Fax Detection for SIP Call and Transfer on Cisco IOS XE

- The Fax Detect feature is supported with routers that are fitted with DSP modules.
- Only the g711ulaw and g711alaw codecs are used for detecting the fax CNG tone.
- Each destination number can be of maximum length of 32 characters.
- Fax Detection is supported with LTI-based transcoding.

Information About Fax Detection for SIP Call and Transfer

Fax detection is typically used if you need to have a single phone number for both voice and fax services. Incoming calls are initially answered by an auto attendant or interactive voice response (IVR) service. At this point, the media stream is monitored for fax tones. Calls identified as coming from a fax machine are then rerouted to a new destination, such as a fax server.

For Fax detection to work, the **cng-fax-detect** command under DSP farm and the **detect-fax** command must be configured in the inbound dial-peer. The fax detection feature may be configured to redirect calls to a local voice port or a remote application.



Note Fax detection on CUBE is also supported through a TCL script. The script answers an incoming call, plays a prompt and makes an outgoing voice or fax call. You can download the TCL script from the [CiscoDevNet Github](#).

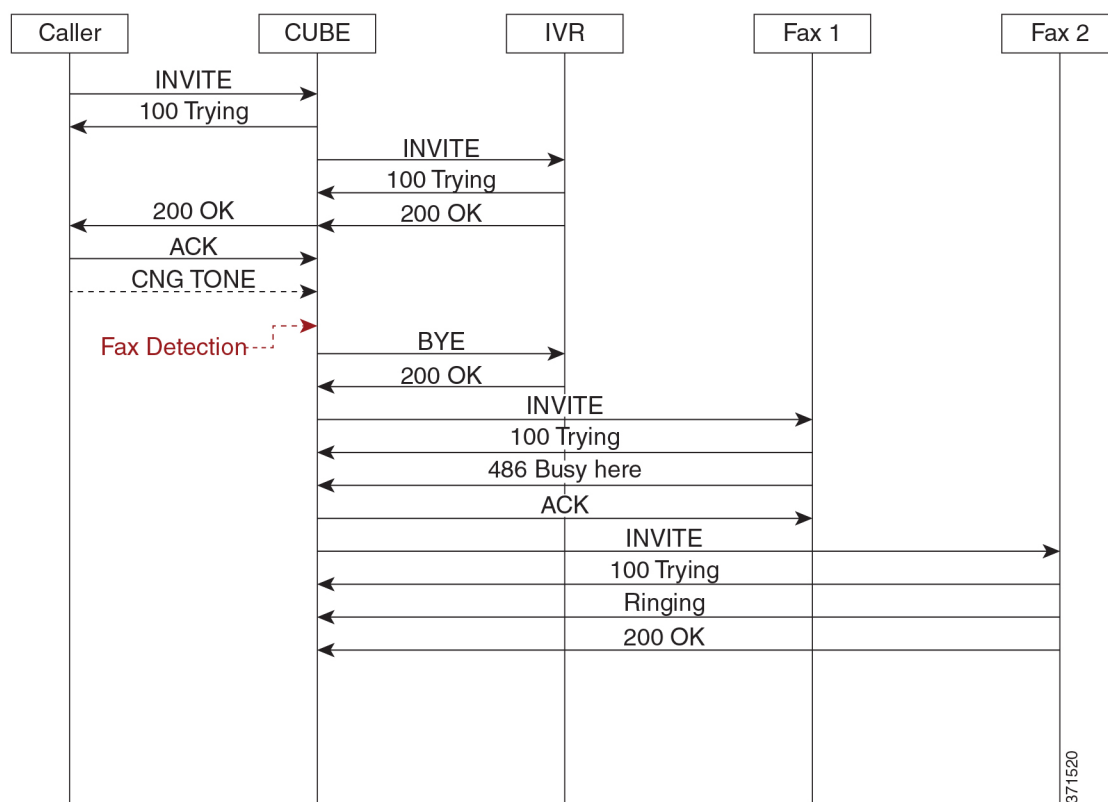


Note If the **silence off** attribute is received in the SDP and the **fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback pass-through {g711alaw | g711ulaw}** codec command is configured, CUBE interprets the received SDP as a fax switchover call.

Local Redirect Mode

Local redirect may be used to transfer a fax call to either a local port or remote destination. Multiple destinations may be used if required, allowing the CUBE to hunt for the first available resource. The configured hunt list can include any number of destination ports.

Figure 34: Local Redirect Call Flow



An initial connection is made as a voice call through CUBE to the IVR. On detection of fax tones in the media path, CUBE closes the connection to the IVR, then hunts through a list of numbers to establish a connection to a fax machine or fax server, allowing the originating fax machine to complete its transmission. In a scenario where T.38 is not supported by CUBE, it will fallback to passthrough.

For each call, a digital signal processor (DSP) channel is allocated to detect the fax CNG tone. This DSP remains allocated until the original call leg clears at the end of the call. In the call flow example above, the first fax machine is busy, so the CUBE establishes the call with the second fax machine.



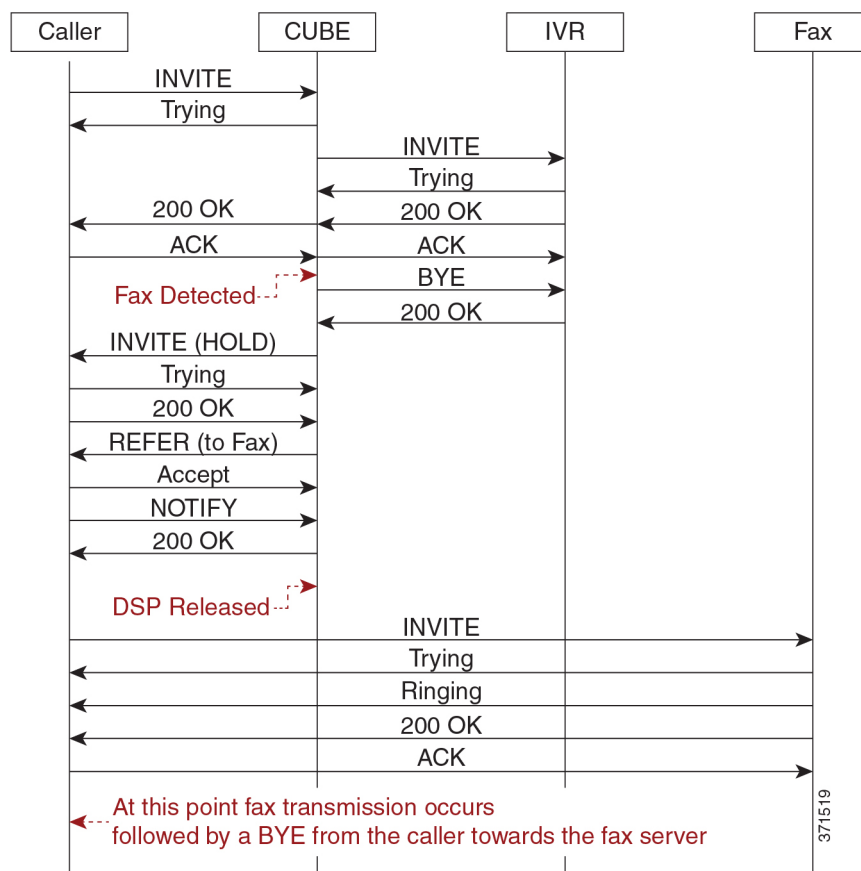
Note For Local Redirect, new calls legs are negotiated as voice, not as fax session.

Refer Redirect Mode

In this mode, calls are redirected to a fax service by the original calling party. The redirect is based on information provided by CUBE in a SIP Refer message (similar to a blind transfer).

In this mode, only one redirection target can be configured.

Figure 35: Refer Redirect Call Flow



An initial connection is made as a voice call through CUBE to the IVR. On detection of fax tones in the media path, CUBE closes the connection to the IVR. To transfer the call, CUBE first sends a re-invite to put the original call leg on hold, then sends a SIP REFER with details of the remote fax server. From this point, CUBE is no longer involved in the call flow as the originating fax communicates directly with the destination server.

For each call, a DSP channel or resource is allocated to detect the CNG tone. This resource is released once the call transfer has been initiated.

Transcoder Behavior for Cisco IOS XE

For the fax tone detection support offered for Cisco IOS XE, the DSP resource behavior for local and refer redirect is as follows:

- For local redirect, CUBE doesn't release the transcoder until the fax call disconnects.
- For refer redirect, CUBE releases the transcoder when the REFER message is sent to the peer leg.

Fax Detection with Cisco IOS XE High Availability

Fax detection and transfer are supported with CUBE High Availability (HA) deployments. In this mode, two CUBE routers are configured to run in Active-Standby mode.

The following behaviors specific to this feature must be noted:

- Failover after initial call has been established, but fax hasn't been detected—The call is preserved, but tone detection is not available for the remainder of that call. The originating fax machine terminates the call after CNG time-out.
- Failover after fax detection, but before the transferred call leg is established—The initial call is preserved and the transfer fails. The originating fax machine terminates the call after CNG time-out.

Fax Detection Configuration for SIP Calls

Configure DSP Resource to Detect Fax Tone

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dspfarm profile *tag* transcode universal**
4. **cng-fax-detect**
5. **maximum sessions *sessions***
6. **associate application CUBE**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dspfarm profile tag transcode universal Example: Device(config)# dspfarm profile 5 transcode universal	Enters DSP farm profile configuration mode and enables the profile for transcoding.
Step 4	cng-fax-detect Example: Device(config-dspfarm-profile)# cng-fax-detect	Enables CNG tone detection.
Step 5	maximum sessions sessions Example: Device(config-dspfarm-profile)# maximum sessions 6	Configures maximum number of sessions.
Step 6	associate application CUBE Example: Device(config-dspfarm-profile)# associate application CUBE	Configures an application to the profile for LTI-based transcoding.
Step 7	end Example: Device(config-dspfarm-profile)# end	Returns to privileged EXEC mode.

Dial-peer Configuration to Redirect Fax Call

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice *number* voip
4. description *tag*
5. session protocol sipv2
6. incoming called number *number*
7. voice-class codec *tag*
8. no vad
9. detect-fax [mode { *refernumber*|*localnumber*}]

10. end

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	dial-peer voice <i>number</i> voip Example: Device(config)# dial-peer voice 401 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 4	description <i>tag</i> Example: Device(config-dial-peer)# description Incoming dial-peer for Fax	Provides a description for the incoming dial-peer for Fax.
Step 5	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures SIP as the session protocol type.
Step 6	incoming called number <i>number</i> Example: Device(config-dial-peer)# incoming called-number 903309	Creates inbound dial-peer.
Step 7	voice-class codec <i>tag</i> Example: Device(config-dial-peer)# voice-class codec 111	Applies the previously configured voice class and associated codecs to a dial peer. The voice class codec can only include g711ulaw and g711alaw.
Step 8	no vad Example: Device(config-dial-peer)# no vad	Disables voice activity detection (VAD) for the calls using the dial peer being configured.
Step 9	detect-fax [<i>mode</i> { <i>refernumber</i> <i>localnumber</i> }] Example:	Defines fax detection as local or refer mode and refers to the directory number of the fax machine.

	Command or Action	Purpose
	Device(config-dial-peer)# detect-fax refer 12101	If local mode is configured, then a list of numbers, separated by a space may be entered. Refer mode only allows a destination number to be configured.
Step 10	end Example: Device(config-dial-peer)# end	Returns to privileged EXEC mode.

Verify Fax Detection Configuration for SIP Calls

SUMMARY STEPS

1. enable
2. show call active voice compact
3. show dspfarm dsp active

DETAILED STEPS

Step 1 enable

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 show call active voice compact

Example:

This is a sample output of call setup when the call is connected:

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

```
<callID>  A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 3
      9   ANS  T4      g711ulaw  VOIP      P808808           9.42.25.145:17940
     10   ORG  T4      g711ulaw  VOIP      P309903           9.42.25.149:16396
     11   ANS  T4      g711ulaw  VOIP      P808808           9.42.25.149:16394
```

Step 3 show dspfarm dsp active

Example:

This is a sample output of the DSP channel reserved to detect CNG tone after the call is set up.

```
Device# show dspfarm dsp active
```

```

SLOT    DSP VERSION  STATUS  CHNL USE  TYPE      RSC_ID  BRIDGE_ID  PKTS_TXED  PKTS_RXED
  0      2    36.1.0   UP       1    USED    xcode      1          9          228        119
```

```

0      2  36.1.0  UP      1  USED  xcode  1      10      113      251
Total number of DSPFARM DSP channel(s) 1

```

Troubleshoot Fax Failures due to Multiple M-Lines on the CUBE

The CUBE doesn't understand multiple m-lines during a voice-to-fax switch-over. To resolve this issue, you can adopt the following workaround using Session Initiation Protocol (SIP) profiles.

Problem

When a provider sends an Invite message to the CUBE during a voice-to-fax switch-over, it includes a Session Description Protocol (SDP) with two m-lines. If the m-lines are in an unexpected format, then the CUBE fails to process it. As a result, it sends a malformed SDP to the fax server in the Invite message. Therefore, all calls fail.

Here is an example of an unaccepted m-line format:

```
m=image
```

```
m=audio
```

Solution

The workaround to troubleshoot fax failures due to multiple m-lines issue:

- Use only one m-line for the voice-to-fax switch-over.
- Use protocol-based pass-through.
- Have the provider place the *m=audio* line above the *m=image* line.
- Use the fax server in order to initiate the switch-over with the use of CNG in a T.30 indicator packet.

The CUBE version 10.0 uses a new feature for inbound SIP profiles. These profiles are applied to inbound SIP messages before it's presented to the SIP stack. The idea behind the use of the inbound SIP profiles in this scenario is to remove the *m=audio* line, so that the CUBE can work with a single *m=image* line.

Here is an example of the re-Invite message when the provider desires to escalate the voice call to fax:

```

Received:
INVITE sip:025027141@192.0.2.2:5060 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1:5060;branch=z9hG4bKnM30rd10dofho0fo9011sb0000g00.1
Call-ID: 6B6CB982-B41D11E3-898F851F-F1ADD198@192.0.2.2
From: <sip:026455288@25027100.xyz>;tag=7qapqh6u-CC-36
To: "Administrator" <sip:025027141@25027100.xyz>;tag=85A6C018-2489
CSeq: 1 INVITE
Contact: <sip:192.0.2.1:5060;transport=udp>
Max-Forwards: 69
Content-Length: 431
Content-Type: application/sdp
v=0
o=HuaweiSoftX3000 22157305 22157306 IN IP4 192.0.2.1
s=Sip Call
c=IN IP4 192.0.2.1
t=0 0
m=image 53200 udpt1 t38
a=T38FaxVersion:0

```

```

a=T38MaxBitRate:14400
a=T38FaxRateManagement:transferredTCF
a=T38FaxUdpEC:t38UDPRedundancy
m=audio 53190 RTP/AVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=silenceSupp:off - - - -
a=ecan:fb on -
a=X-fax

```

This SIP profile configuration can be applied in order to remove the *m=audio* line:

```

voice class sip-profiles 966
request REINVITE sdp-header Audio-Media modify "(.*)" "a=sendrecv"
voice service voip
sip
voice-class sip profiles 966 inbound
or
dial-peer voice XYZ voip
voice-class sip profiles 966 inbound

```

The SIP profile changes the *m=audio* line to *a=sendrecv*, which acts as a line in the SDP that isn't relevant. This allows the CUBE to send a re-Invite message to the fax server and await the *200 OK* response.

When sending a *200 OK* message as a response to the received re-Invite, it includes both m-lines that adhere to RFC standards. The response message contains the same number of media attributes as the offer message.

This can be accomplished using a standard outbound SIP profile that is applied on the dial-peer of the provider:

```

voice class sip-profiles 200
response 200 method re-invite sdp-header Attribute modify "t38UDPRedundancy"
  "t38UDPRedundancy\x0D\x0Am=audio 0 RTP/AVP"

```

Replace the *"t38UDPRedundancy"* to ensure that the re-Invite with multiple m-lines is correctly handled and the response to the provider is RFC-compliant:

```

"t38UDPRedundancy"
New line ( \x0D\x0A )
m=audio 0 RTP/AVP

```

In order to resolve the issue of multiple m-lines, employ the workarounds that are discussed (most of which are provider-dependent). Also, it's observed that the Xmedius Server can initiate the switch-over, as it forces the server to send the T.38 re-Invite message avoiding multiple m-lines.

Fax Detection Troubleshooting for SIP Calls

You can enable the logs of the following **debug** or **show** commands, which are helpful in debugging fax detection for SIP calls:

- **debug voip ipipgw all**
- **debug ccsip verbose**
- **debug voip ccapi all**
- **debug voip dsmp all**
- **debug voip hpi all**
- **debug media resource provisioning all**

- **show call active voice compact**
- **show dspfarm dsp active**
- **show voip rtp connections**

Configuration Examples for Fax Detection for SIP Calls

Example: Configuring Local Redirect

The following is a sample configuration in local redirect mode for fax detection. In this example, the dial-peer has to be configured for the FAX directory numbers 9033010 and 9033011.

```
dspfarm profile 10 transcode universal
  codec g729abr8
  codec g729ar8
  codec g711alaw
  codec g711ulaw
  codec g729r8
  codec ilbc
  codec g722-64
  cng-fax-detect
  maximum sessions 6
  associate application CUBE
!
dial-peer voice 401 voip
  description "Incoming dial-peer to ASR"
  session protocol sipv2
  incoming called-number 903309
  voice-class codec 111
  dtmf-relay rtp-nte
  no vad
  detect-fax mode local 9033010 9033011

dial-peer voice 406 voip
  description "Outbound dialpeer for ..."
  destination-pattern 9033010
  session protocol sipv2
  session target ipv4:9.41.36.11:14762
  voice-class codec 111
  dtmf-relay rtp-nte
  fax protocol pass-through g711ulaw
  no vad

dial-peer voice 406 voip
  description "Outbound dialpeer for ..."
  destination-pattern 9033011
  session protocol sipv2
  session target ipv4:9.41.36.11:14765
  voice-class codec 111
  dtmf-relay rtp-nte
  fax protocol pass-through g711ulaw
  no vad
```

Example: Configuring Refer Redirect

In Refer mode, only one fax number can be configured.

```
dial-peer voice 401 voip
description "Incoming dial-peer to ASR"
session protocol sipv2
incoming called-number 903309
voice-class codec 111
dtmf-relay rtp-nte
no vad
detect-fax mode refer 9033010
```

```
dial-peer voice 406 voip
description "Outbound dialpeer for ..."
destination-pattern 9033010
session protocol sipv2
session target ipv4:9.41.36.11:14762
voice-class codec 111
dtmf-relay rtp-nte
fax protocol pass-through g711ulaw
no vad
```



CHAPTER 47

Video Suppression

- [Video Suppression, on page 441](#)
- [Feature Information for Video Suppression, on page 441](#)
- [Restrictions, on page 442](#)
- [Information About Video Suppression, on page 442](#)
- [Configuring Video Suppression, on page 442](#)
- [Troubleshooting Tips, on page 443](#)

Video Suppression

The video suppression feature allows pass-through of only audio and image (for T.38 Fax) media types in SDP and drops all other media capabilities.

Feature Information for Video Suppression

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 68: Feature Information for Video Suppression

Feature Name	Releases	Feature Information
Support for Video Suppression	Cisco IOS 15.6(2)T Cisco IOS XE Denali 16.3.1	This feature allows pass-through of only audio and application (for T.38 Fax) media types and drops all other media types in SDP. The following commands are introduced: audio forced , voice-class sip audio forced

Restrictions

- Supports only SIP-SIP calls.
- Video suppression is not supported in SDP pass-through mode.
- Video suppression feature removes both video and application m-lines in the incoming SDP. It is not possible to remove application m-line alone and pass across video m-line parameters.

Information About Video Suppression

Video suppression feature enables CUBE to interwork with the networks that support only audio and image media types in SDP and the networks that support video and application media types in addition to audio and image media types.

By default video suppression feature is disabled on CUBE and hence the video capabilities are passed through in SDP. Passing across the video capabilities could cause interoperability issues if one of the networks do not support video capabilities.

By enabling video suppression feature, you can configure CUBE to pass-through audio and image only, and drop all other capabilities such as video and application m-lines. This helps enterprises to interwork with audio capable networks and video capable networks smoothly.

You can enable video suppression at dial-peer level and at global configuration level.

Feature Behavior

- If video suppression is enabled on any of the dial-peers (inbound or outbound), video capabilities are not offered for that particular call.
- Configuring **voice-class sip audio forced [system]** command at a dial-peer level makes use of global configuration level settings for allowing only audio and image media.
- Video suppression feature will work as expected even when codec transparent feature is configured.

Configuring Video Suppression

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - In the dial-peer configuration mode
voice-class sip audio forced
 - In the global VoIP SIP configuration mode
audio forced

4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • In the dial-peer configuration mode voice-class sip audio forced • In the global VoIP SIP configuration mode audio forced <p>Example: In dial-peer configuration mode</p> <pre>!Applying audio-forced to one dial peer only Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip audio forced Device (config-dial-peer)# end</pre> <p>Example: In global VoIP SIP configuration mode</p> <pre>! Applying audio forced globally Device(config)# voice service voip Device (config-voi-serv)# sip Device (config-voi-sip)# audio forced Device (config-voi-sip)# end</pre>	Enables pass-through of only audio and image media types in SDP.
Step 4	end	Exits present configuration mode and enters privileged EXEC mode.

Troubleshooting Tips

The following commands are useful for debugging:

- show voip rtp connections
- show call active voice brief
- show call active video brief
- debug voip dialpeer
- debug ccsip all

- debug voip ccapi inout



CHAPTER 48

ICE-Lite Support

- [ICE-Lite Support on CUBE, on page 445](#)
- [Restrictions for ICE-lite Support, on page 447](#)
- [Configure ICE-Lite, on page 448](#)
- [Verify ICE-Lite \(Success Flow Calls\), on page 449](#)
- [Error Flow Calls, on page 452](#)
- [Configuration Example, on page 457](#)
- [Troubleshoot ICE-Lite Support, on page 457](#)
- [Additional References, on page 458](#)

ICE-Lite Support on CUBE

Interactive Connectivity Establishment (ICE) is a protocol for Network Address Translator (NAT) traversal for UDP-based multimedia sessions established with the offer-answer model. ICE makes use of the Session Traversal Utilities for NAT (STUN) protocol and its extension, Traversal Using Relay NAT (TURN), and can be used by any protocol utilizing the offer-answer model, such as the Session Initiation Protocol (SIP).

The ICE-Lite Support on CUBE feature enables the remote peers of CUBE (that may be behind a NAT and doing ICE) to use the ICE semantics in the session description protocol (SDP) and perform an offer-answer exchange of SDP messages. The CUBE can also interwork with endpoints that support or do not support ICE. ICE agents (devices) that are always attached to the public Internet have a special type of implementation called Lite. CUBE will be in ICE-lite mode only. CUBE supports the ICE-lite feature from Cisco IOS Release 15.5(2)S.

Feature Information

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 69: Feature Information for ICE-Lite Support on CUBE

Feature Name	Releases	Feature Information
ICE-Lite Support on CUBE	Cisco IOS 15.5(3)M Cisco IOS XE 3.16S	The ICE-Lite Support on CUBE feature enables the remote peers of CUBE (that may be behind a NAT and doing ICE) to use the ICE semantics in the session description protocol (SDP) and perform an offer-answer exchange of SDP messages. The CUBE can also interwork with endpoints that support or do not support ICE. ICE agents (devices) that are always attached to the public Internet have a special type of implementation called Lite. CUBE will be in ICE-lite mode only. The following commands were introduced or modified: debug voip icelib , show voip ice global-stats , show voip ice instance call-id call-id , show voip ice summary , and stun usage ice

Characteristics

The following are some of the key characteristics of ICE-lite.

- A CLI configured for ICE-lite.
- Support for ICE-lite in the contact header with a media-tag option of REGISTER message (as per RFC 5768).
- ICE-lite feature is in compliance with section 4.2 of RFC 7584, with CUBE acting as ICE termination Back-to-Back UA.
- CUBE accepts Full ICE Offer and responds in ICE-lite mode.
- CUBE responds to mid call updates or early dialog updates with changes to SDP parameters, and which requires ICE to restart.
- For outbound offer from CUBE, a Session Description Protocol (SDP) with ICE-lite semantics is sent.
- ICE protocol verifies all types of media streams (audio, video, application media lines) and components (RTP, RTCP), wherever applicable.

ICE Candidate

To execute ICE, an agent has to identify all of its address candidates. A candidate is a transport address—a combination of IP address and port for a transport protocol, such as UDP. A candidate can be derived from physical or logical network interfaces, or discoverable using STUN and TURN. A viable candidate is a transport address obtained directly from a local interface; such a candidate is called a host candidate. The local interface could be ethernet or WiFi, or it could be one that is obtained through a tunnel mechanism, such as a Virtual Private Network (VPN) or Mobile IP (MIP). In all cases, such a network interface appears to the agent as a local interface from which ports (and thus candidates) can be allocated.



Note Refer to RFC 5245 for more information about ICE candidates.

ICE Lite

ICE agents (devices) that are always attached to the public Internet have a special type of implementation called Lite. For ICE to be used in a call, both the endpoints (agents) must support it. An ICE agent that supports Lite neither gathers ICE candidates nor triggers ICE connectivity checks; however, the agent responds to connectivity checks and includes only host candidates for any media stream. An ICE agent that supports the lite mode is called an ICE-lite endpoint.



Note Refer to RFC 5245 for more information about ICE-lite implementation and connectivity checks.

High Availability Support with ICE

High availability (HA) is supported only for audio calls that use ICE. For video calls, as the size of SDP is larger, HA will not work. Some of the design considerations are the following:

- No new checkpoint module for ICE instance.
- ICE instance will be re-created on the standby device from SIP HA re-creation path by using source SDP, destination SDP, and configuration profile.
- As no information related to ICE is checkpointed, in the standby device, the ICE valid list (created after connectivity checks are done) is populated from currently used media address.

Restrictions for ICE-lite Support

The following features are not supported with ICE:

- IPv6
- Alternative Network Address Types (ANAT)
- ANAT-ICE interworking
- Media anti-trombone
- High availability support for video calls
- Codec Transparent
- SDP passthrough
- Media flow-around
- Resource Reservation Protocol (RSVP)
- SIP-to-TDM gateway support



Note A workaround option for ICE-lite based media optimization is to configure loopback dial-peer on a TDM gateway. Contact Account or TAC teams for further technical details.

- Media Termination Point (MTP)
- VXML and TCL Scripts

Configure ICE-Lite

ICE lite can be configured under STUN, and the decision to use ICE for a session is based on the offer/answer. This configuration is used for outbound dial-peers of CUBE to decide whether to offer ICE in SDP or not. For an incoming offer, the decision to do ICE is based on what the remote end offers in SDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class stun-usage tag**
4. **stun usage ice lite**
5. **end**

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	voice class stun-usage tag Example: Device(config)# voice class stun-usage 5	Sets STUN usage global parameters, and enters voice class configuration mode.
Step 4	stun usage ice lite Example: Device(config-class)# stun usage ice lite	Configures ICE in ICE-Lite mode.
Step 5	end Example: Device(config-class)# end	Returns to privileged EXEC mode.

Verify ICE-Lite (Success Flow Calls)

The following **show** commands can be used to verify ICE for success flow calls. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **show call active video compact**
2. **show voip rtp connections**
3. **show voip ice instance call-id** *call-id-1*
4. **show voip ice instance call-id** *call-id-2*
5. **show voip ice summary**
6. **show voip ice global-stats**

DETAILED STEPS

Step 1 show call active video compact

Example:

```
Device# show call active video compact
```

```
<callID>  A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 4
          25 ANS   T189   H264      VOIP-VIDEO P8181    72.163.212.137:2328
          30 ORG   T189   H264      VOIP-VIDEO P9191     9.45.46.16:8028
          35 ANS   T189   H264      VOIP-VIDEO P8181     9.45.46.16:8008
          36 ORG   T189   H264      VOIP-VIDEO P9191    72.163.212.163:2328
```

Step 2 show voip rtp connections

The following sample output displays the VoIP RTP usage information and RTP active connections.

Example:

```
Device# show voip rtp connections
```

```
VoIP RTP Port Usage Information:
```

```
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 20
```

Media-Address Range	Min Port	Max Port	Ports Available	Ports Reserved	Ports In-use
Global Media Pool	8000	48198	19999	101	20

```
VoIP RTP active connections :
```

No.	CallId	dstCall	LocalRTP	RmtRTP	LocalIP	RemoteIP	MPSS
1	25	30	8000	2326	10.104.45.107	72.163.212.137	NO
2	26	31	8002	2328	10.104.45.107	72.163.212.137	NO
3	27	32	8036	2454	10.104.45.107	72.163.212.137	NO
4	28	33	8004	2330	10.104.45.107	72.163.212.137	NO
5	29	34	8038	2332	10.104.45.107	72.163.212.137	NO
6	30	25	8006	8016	9.45.46.16	9.45.46.16	NO
7	31	26	8008	8028	9.45.46.16	9.45.46.16	NO
8	32	27	8010	8030	9.45.46.16	9.45.46.16	NO
9	33	28	8012	8032	9.45.46.16	9.45.46.16	NO

```

10 34 29 8014 8034 9.45.46.16 9.45.46.16 NO
11 35 36 8016 8006 9.45.46.16 9.45.46.16 NO
12 36 35 8018 2326 10.104.45.107 72.163.212.163 NO
13 37 41 8020 2328 10.104.45.107 72.163.212.163 NO
14 38 42 8022 2454 10.104.45.107 72.163.212.163 NO
15 39 43 8024 2330 10.104.45.107 72.163.212.163 NO
16 40 44 8026 2332 10.104.45.107 72.163.212.163 NO
17 41 37 8028 8008 9.45.46.16 9.45.46.16 NO
18 42 38 8030 8010 9.45.46.16 9.45.46.16 NO
19 43 39 8032 8012 9.45.46.16 9.45.46.16 NO
20 44 40 8034 8014 9.45.46.16 9.45.46.16 NO
Found 20 active RTP connections

```

Step 3 `show voip ice instance call-id call-id-1`

The following sample output displays the active ICE sessions on the ICE-full and the ICE-lite legs where there are ICE negotiations.

Example:

```
Device# show voip ice instance call-id 25
```

```
Interactive Connectivity Check(ICE) Instance details:
```

```
Call-ID is 25
```

```
Instance is 0x7FC617FC0508
```

```
Overall ICE-State is COMPLETED
```

```
LocalAgent's mode is ICE-CONTROLLED
```

```
RemoteAgent's mode is ICE-CONTROLLING
```

```
m-line:1
```

```
-----
```

```
ICE-State: ACTIVE
```

```
NominatedPairs:
```

```
LocalIP 10.104.45.107 port 8000 type host RemoteIP 72.163.212.137 port 2326 type host
```

```
m-line:2
```

```
-----
```

```
ICE-State: ACTIVE
```

```
NominatedPairs:
```

```
LocalIP 10.104.45.107 port 8002 type host RemoteIP 72.163.212.137 port 2328 type host
```

```
LocalIP 10.104.45.107 port 8003 type host RemoteIP 72.163.212.137 port 2329 type host
```

```
m-line:3
```

```
-----
```

```
ICE-State: ACTIVE
```

```
NominatedPairs:
```

```
LocalIP 10.104.45.107 port 8036 type host RemoteIP 72.163.212.137 port 2454 type host
```

```
m-line:4
```

```
-----
```

```
ICE-State: ACTIVE
```

```
NominatedPairs:
```

```
LocalIP 10.104.45.107 port 8004 type host RemoteIP 72.163.212.137 port 2330 type host
```

```
LocalIP 10.104.45.107 port 8005 type host RemoteIP 72.163.212.137 port 2331 type host
```

```
m-line:5
```

```
-----
```

```
ICE-State: ACTIVE
```

```
NominatedPairs:
```

```
LocalIP 10.104.45.107 port 8038 type host RemoteIP 72.163.212.137 port 2332 type host
```

```
Total Rx STUN Bind Req 22
```

```
Total Tx STUN Bind Succ Resp 22
```

```
Total Tx STUN Bind failure resp 0
```

Step 4 **show voip ice instance call-id** *call-id-2*

The following sample output displays the idle ICE sessions on the ICE-lite and the ICE-lite legs where there are no ICE negotiations.

Example:

```
Device# show voip ice instance call-id 30

Interactive Connectivity Check(ICE) Instance details:
Call-ID is 30
Instance is 0x7FC617FC03F8
Overall ICE-State is RUNNING
LocalAgent's mode is ICE-CONTROLLED
RemoteAgent's mode is ICE-CONTROLLING
m-line:1
-----
ICE-State: IDLE
No candidate has been nominated

m-line:2
-----
ICE-State: IDLE
No candidate has been nominated

m-line:3
-----
ICE-State: IDLE
No candidate has been nominated

m-line:4
-----
ICE-State: IDLE
No candidate has been nominated

m-line:5
-----
ICE-State: IDLE
No candidate has been nominated

Total Rx STUN Bind Req 0
Total Tx STUN Bind Succ Resp 0
Total Tx STUN Bind failure resp 0
```

Step 5 **show voip ice summary**

The following sample output displays a summary of active ICE sessions.

Example:

```
Device# show voip ice summary

CALL-ID          ICE-STATE
-----
25                COMPLETED
30                RUNNING
35                RUNNING
36                COMPLETED
```

Step 6 **show voip ice global-stats**

The following sample output displays the global ICE statistics.

Example:

```
Device# show voip ice global-stats

Interactive Connectivity Establishment(ICE) global stats:
Total Rx Stun BindingRequests      : 43
Total Tx Stun BindingSuccessResponses: 43
Total Tx Stun BindingErrorResponses : 0
```

Error Flow Calls

The following are the **show** command sample outputs followed by the system logs for error flow calls. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **show call active voice compact**
2. **show voip rtp connections**
3. **show voip ice instance call-id *call-id***
4. **show voip ice instance call-id *call-id***
5. **show voip ice summary**
6. **show voip ice global-stats**

DETAILED STEPS

Step 1 show call active voice compact

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
          57 ANS   T4      g711ulaw  VOIP      Padithyam         173.39.64.79:7078
          58 ORG   T4      g711ulaw  VOIP      P9191             72.163.212.163:2336
```

Step 2 show voip rtp connections

The following sample output displays the VoIP RTP usage information and RTP active connections.

Example:

```
Device# show voip rtp connections

VoIP RTP Port Usage Information:
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 2

Media-Address Range      Min   Max   Ports   Ports   Ports
                          Port  Port Available Reserved In-use
-----
Global Media Pool        8000 48198 19999   101     2
-----
VoIP RTP active connections :
```

```

No. CallId dstCallLocalRTP RmtRTP LocalIP RemoteIP MPSS
1 57 58 8040 7078 10.104.45.107 173.39.64.79 NO
2 58 57 8042 2336 10.104.45.107 72.163.212.163 NO
Found 2 active RTP connections

```

Step 3 `show voip ice instance call-id` *call-id*

The following sample output displays the ICE sessions.

Example:

```

Device# show voip ice instance call-id 57

Interactive Connectivity Check(ICE) Instance details:
Call-ID is 57
Instance is 0x7FC617FC03F8
Overall ICE-State is RUNNING
LocalAgent's mode is ICE-CONTROLLED
RemoteAgent's mode is ICE-CONTROLLING
m-line:1
-----
ICE-State: IDLE
No candidate has been nominated

Total Rx STUN Bind Req 2
Total Tx STUN Bind Succ Resp 0
Total Tx STUN Bind failure resp 2

```

Step 4 `show voip ice instance call-id` *call-id*

The following sample output displays the ICE sessions.

Example:

```

Device# show voip ice instance call-id 58

Interactive Connectivity Check(ICE) Instance details:
Call-ID is 58
Instance is 0x7FC617FC0508
Overall ICE-State is RUNNING
LocalAgent's mode is ICE-CONTROLLED
RemoteAgent's mode is ICE-CONTROLLING
m-line:1
-----
ICE-State: IDLE
No candidate has been nominated

Total Rx STUN Bind Req 2
Total Tx STUN Bind Succ Resp 0
Total Tx STUN Bind failure resp 2

```

Step 5 `show voip ice summary`

The following sample output displays a summary of active ICE sessions.

Example:

```

Device# show voip ice summary

CALL-ID          ICE-STATE
-----
57                RUNNING

```

```
58                                RUNNING
Total number of sessions: 2
```

Step 6 show voip ice global-stats

The following sample output displays the global ICE statistics.

Example:

```
Device# show voip ice global-stats

Interactive Connectivity Establishment(ICE) global stats:
Total Rx Stun BindingRequests      : 47
Total Tx Stun BindingSuccessResponses: 43
Total Tx Stun BindingErrorResponse : 4
```

The following are the sys logs for invalid message integrity and for sending ICE-controlled parameter.

Sys Log for invalid message integrity:

```
004012: *Aug  8 14:25:30.876 IST: %CISCO_STUN-4-INVALID_MESSAGE_INTEGRITY: Invalid Message-Integrity
attribute in the received STUN message on UDP IP address 10.104.45.107 port 8040###STUN Message
structure start###
Message Type           : STUN_MSG_TYPE_BINDING_REQ
Magic Cookie          : 2112A442
Transaction ID        : 01CD61B24C077331EDC27A5B
Mapped Address        : Not Set/Present
User Name             : Not Set/Present
Error code not present
Alternate Server       : Not Set/Present
Realm                 : Not Set/Present
nonce                 : Not Set/Present
Xormapped Address     : Not Set/Present
Server                : Not Set/Present
ICE Priority           : Not Set/Present
ICE Controlled        : Not Set/Present
ICE Controlling       : Not Set/Present
Cisco-flowdata        :
cisco-flowdata is not present
Message Integrity     : Not Set/Present
Finger Print          : Not Set/Present
###STUN Message structure End###

004013: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/cisco_stun_process_event: Exit
004014: *Aug  8 14:25:30.876 IST: //57/91300134802E/STUN/Inout/cisco_stun_process_event: Entry with
Eventtype:7
004015: *Aug  8 14:25:30.876 IST: //57/91300134802E/STUN/Inout/cisco_stun_process_send_msg_event:
Entry
004016: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSendMsg: Entry
004017: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunGetMsgClass: Entry
004018: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunGetMsgClass: en_StunResp
004019: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSendMsg: dMsgClass:3
004020: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeMsg: Entry
004021: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunCalculateSize:      Length of
ERROR-CODE = 20
004022: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunCalculateSize:      Length of
MESSAGE-INTEGRITY = 24
004023: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsg: STUN Message Length
= 64
004024: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeHdr: Entry
004025: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeHdr: Exit
004026: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeAttr: Entry
004027: *Aug  8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeAttr: Exit
```



```

004028: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsgIntegrity: Original
STUN Message Length = 44
004029: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsgIntegrity: Adjusted
STUN Message Length = 44
004030: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsgIntegrity: Successfully
Encoded MI attribute. Exit
004031: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSetMsgIntegrityToStunMessage:
Entry
004032: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSetMsgIntegrityToStunMessage: Exit
with success
004033: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsg: Total length:64
004034: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeMsg: Exit
004035: *Aug 8 14:25:30.876 IST: //57/91300134802E/STUN/Inout/stunSendMsgToNetwork: Entry
004036: *Aug 8 14:25:30.876 IST: //57/91300134802E/STUN/Detail/stunSendMsgToNetwork: Message sending
from, 10.104.45.107:8040, to 173.39.64.79:7078
004037: *Aug 8 14:25:30.876 IST: //57/91300134802E/STUN/Detail/stunSendMsgToNetwork: Stun Message:

0111002C2112A44201CD61B24C077331EDC27A5B0009000F0000040042616420526571756573740000080014D0E2E828944BF3D07CC5C06D026D8909B85EF3E9
004038: *Aug 8 14:25:30.876 IST: //57/91300134802E/STUN/Inout/stunSendMsgToNetwork: Exit
004039: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSendMsg:
** Sent Stun Packet to Network **
###STUN Message structure start###
Message Type : STUN_MSG_TYPE_BINDING_ERR_RESP
Magic Cookie : 2112A442
Transaction ID : 01CD61B24C077331EDC27A5B
Mapped Address : Not Set/Present
User Name : Not Set/Present
Error Code : Number = 400 ,Reason = Bad Request
Alternate Server : Not Set/Present
Realm : Not Set/Present
nonce : Not Set/Present
Xormapped Address : Not Set/Present
Server : Not Set/Present
ICE Priority : Not Set/Present
ICE Controlled : Not Set/Present
ICE Controlling : Not Set/Present
Cisco-flowdata :
cisco-flowdata is not present
Message Integrity : D0E2E828944BF3D07CC5C06D026D8909B85EF3E9
004040: *Aug 8 14:25:30.876 IST: Finger Print : Not Set/Present
###STUN Message structure End###

004041: *Aug 8 14:25:30.876 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSendMsg: Sent Bind Response, Free
the transaction
004042: *Aug 8 14:25:30.876 IST: //57/91300134802E/STUN/Detail/cisco_stun_process_send_msg_event:
STUN message Sent

```

Sys Log for sending ICE-controlled parameter instead of ICE-controlling parameter:

```

004130: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunGetMsgClass: Entry
004131: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunGetMsgClass: en_StunReq
004132: *Aug 8 14:25:30.912 IST: %CISCO_STUN-4-ICE_ROLE_CONFLICT: Ice Role Conflcit detected in the
received STUN message on UDP IP address 10.104.45.107 port 8042
004133: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSetErrorCodeToStunMessage: Entry
004134: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSetErrorCodeToStunMessage:
reason:Role Conflcit, code:487
004135: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSetErrorCodeToStunMessage: Exit
with success
004136: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stun_process_send_bind_response: Exit
004137: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stun_post_bind_request_ind_to_app:
Post Message to Application
004138: *Aug 8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/cisco_stun_process_stun_pak_rcvd_event:
Received New STUN message###STUN Message structure start###
Message Type : STUN_MSG_TYPE_BINDING_REQ

```

Error Flow Calls

```

Message Length           : 80
Magic Cookie             : 2112A442
Transaction ID           : F1CF84958CE76D15C83059D9
Mapped Address           : Not Set/Present
User Name                : GAah:4wWY
Error code not present
Alternate Server         : Not Set/Present
Realm                   : Not Set/Present
nonce                   : Not Set/Present
Xormapped Address       : Not Set/Present
Server                  : Cisco
ICE Priority             : 1862270975
ICE Controlled         : 11920035603547232620
ICE Controlling       : Not Set/Present
Cisco-flowdata          :
cisco-flowdata is not present
Message Integrity        : 0AF4B8C2378CB90AB0BA3806507D766BF5CD1DD
004139: *Aug  8 14:25:30.912 IST: Finger Print           : 4235512547
###STUN Message structure End###

004140: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/cisco_stun_process_event: Exit
004141: *Aug  8 14:25:30.912 IST: //58/91300134802E/STUN/Inout/cisco_stun_process_event: Entry with
      EventType:7
004142: *Aug  8 14:25:30.912 IST: //58/91300134802E/STUN/Inout/cisco_stun_process_send_msg_event:
      Entry
004143: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSendMsg: Entry
004144: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunGetMsgClass: Entry
004145: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunGetMsgClass: en_StunResp
004146: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSendMsg: dMsgClass:3
004147: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeMsg: Entry
004148: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunCalculateSize:      Length of
      ERROR-CODE = 24
004149: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunCalculateSize:      Length of
      MESSAGE-INTEGRITY = 24
004150: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsg: STUN Message Length
      = 68
004151: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeHdr: Entry
004152: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeHdr: Exit
004153: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeAttr: Entry
004154: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeAttr: Exit
004155: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsgIntegrity: Original
      STUN Message Length = 48
004156: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsgIntegrity: Adjusted
      STUN Message Length = 48
004157: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsgIntegrity: Successfully
      Encoded MI attribute. Exit
004158: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSetMsgIntegrityToStunMessage:
      Entry
004159: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunSetMsgIntegrityToStunMessage: Exit
      with success
004160: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunEncodeMsg: Total length:68
004161: *Aug  8 14:25:30.912 IST: //-1/xxxxxxxxxxxxx/STUN/Inout/stunEncodeMsg: Exit
004162: *Aug  8 14:25:30.912 IST: //58/91300134802E/STUN/Inout/stunSendMsgToNetwork: Entry
004163: *Aug  8 14:25:30.912 IST: //58/91300134802E/STUN/Detail/stunSendMsgToNetwork: Message sending
      from, 10.104.45.107:8042, to 72.163.212.163:2336
004164: *Aug  8 14:25:30.912 IST: //58/91300134802E/STUN/Detail/stunSendMsgToNetwork: Stun Message:

011100302112A442F1CF84958CE76D15C83059D9000900110000457526F6C6520436F6E666C636974000000008001413402FC99C60296539026305739773476578806E
004165: *Aug  8 14:25:30.913 IST: //58/91300134802E/STUN/Inout/stunSendMsgToNetwork: Exit
004166: *Aug  8 14:25:30.913 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSendMsg:
** Sent Stun Packet to Network **
###STUN Message structure start###
Message Type           : STUN_MSG_TYPE_BINDING_ERR_RESP
Magic Cookie             : 2112A442

```

```

Transaction ID           : F1CF84958CE76D15C83059D9
Mapped Address          : Not Set/Present
User Name               : Not Set/Present
Error Code             : Number = 487 ,Reason = Role Conflcit
Alternate Server        : Not Set/Present
Realm                   : Not Set/Present
nonce                   : Not Set/Present
Xormapped Address       : Not Set/Present
Server                  : Not Set/Present
ICE Priority             : Not Set/Present
ICE Controlled          : Not Set/Present
ICE Controlling         : Not Set/Present
Cisco-flowdata         :
cisco-flowdata is not present
Message Integrity       : 13402FC99C60296539026305739773476578806E
004167: *Aug  8 14:25:30.913 IST: Finger Print                : Not Set/Present
###STUN Message structure End###

004168: *Aug  8 14:25:30.913 IST: //-1/xxxxxxxxxxxxx/STUN/Detail/stunSendMsg: Sent Bind Response, Free
the transaction
004169: *Aug  8 14:25:30.913 IST: //58/91300134802E/STUN/Detail/cisco_stun_process_send_msg_event:
STUN message Sent

```

Configuration Example

The following is a sample loopback dial-peer configuration on TDM gateway to support ICE-lite based media optimization:

Troubleshoot ICE-Lite Support

You can use the following **debug** commands to troubleshoot the ICE-lite support on CUBE feature. Use these commands to enable ICE debugs for each call.

- **debug voip icelib all**
- **debug voip icelib default**
- **debug voip icelib detail**
- **debug voip icelib error**
- **debug voip icelib event**
- **debug voip icelib inout**
- **debug voip stun all**
- **debug voip stun default**
- **debug voip stun detail**
- **debug voip stun error**
- **debug voip stun event**

- debug voip stun inout
- debug voip stun message
- debug voip stun packet

Additional References

Standards and RFCs

Standard/RFC	Title
RFC 5389	<i>Session Traversal Utilities for NAT (STUN)</i>
RFC 5245	<i>Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols</i>
RFC 5766	<i>Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)</i>
RFC 5768	<i>Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)</i>
RFC 3840	<i>Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)</i>
RFC 7584	<i>Session Traversal Utilities for NAT (STUN) Message Handling for SIP Back-to-Back User Agents (B2BUAs)</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



CHAPTER 49

NAT Traversal using RTP Keepalive

- [Information about NAT Traversal using Media Keepalives, on page 459](#)
- [Restrictions, on page 461](#)
- [Configure NAT Traversal using Media Keepalive, on page 461](#)
- [Verify NAT Traversal using Media Keepalive Configuration, on page 463](#)
- [Configuration Example, on page 464](#)

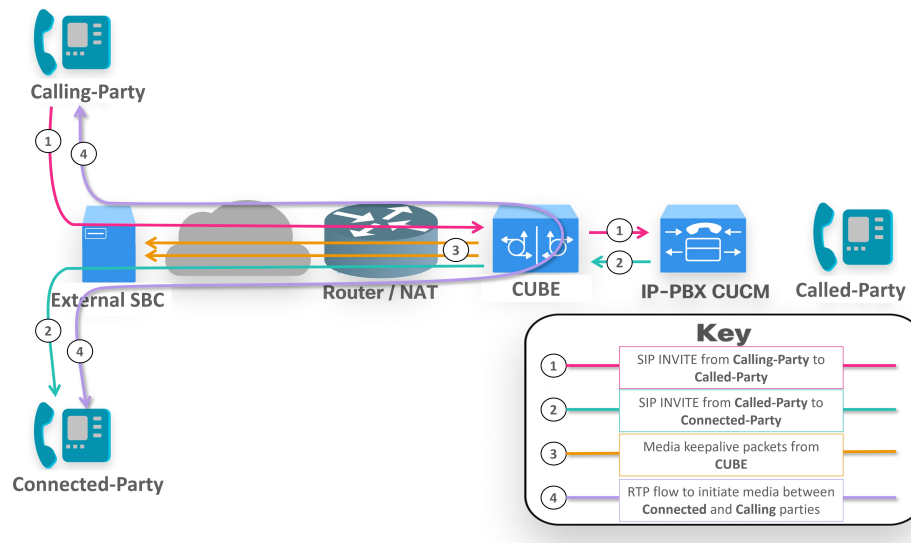
Information about NAT Traversal using Media Keepalives

Network Address Translation (NAT) allows multiple hosts to connect to the internet using a single public IP address. However, for voice calls, NAT bindings must be constantly maintained to ensure uninterrupted media transmission using a keepalive mechanism. Therefore, establishing communication between hosts with NAT-based routers can become challenging. In certain call scenarios, when calls are redirected back to the IP-based Public Switched Telephone Network (PSTN), it's possible that no audio or media is detected. This occurs when both parties involved in the call are located outside of the NAT environment.

Using the media keepalive feature, CUBE deployed behind NAT can send empty media keepalive packets. An empty media keepalive packet refers to a media packet that doesn't contain any payload but only includes the RTP headers. These packets serve the purpose of maintaining the NAT bindings and allowing the peer entity outside of the NAT to perform the media latching required to establish bidirectional media flow. Media latching refers to the method of using the Natted IP address and port of incoming packets as the destination for the packets transmitted in the reverse direction. This feature enables media latching as a solution for NAT traversal without the need for STUN.

CUBE sends periodic media keepalive packets in separate and independent streams, without merging with the negotiated media streams. This approach ensures that the keepalive packets don't interfere with the existing media stream established during the call, allowing for reliable detection of connectivity and end to end media integrity.

Figure 36: CUBE sending Media Keepalive Packets



Periodic media keepalive packets keep pinholes open to allow media communication between the calling party and the connected party. CUBE sends keepalive packets at regular intervals to maintain the NAT bindings for the media. When initially receiving packets from the NAT router, the external network associates the public IP address with the source IP and port. Subsequent media packets are then sent to this associated IP and port. CUBE triggers media keepalive packets without altering the media stream, ensuring the flow of media communication.

Feature Information

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 70: Feature Information of NAT Traversal using Media Keepalives

Feature Name	Releases	Feature Information
NAT Traversal using Media Keepalives	Cisco IOS XE Dublin 17.12.2 Cisco IOS XE 17.13.1a	This feature enables the CUBE to periodically send media keepalive packets, which helps maintain open pinholes and ensures the necessary network bindings for media transmission in a NAT environment.

Media Keepalive Characteristics

The following are the CUBE characteristics for NAT traversal functionality using media keepalive:

- CUBE sends media keepalive packets for each media stream, irrespective of the stream's activity status (inactive, send only, recv only, or sendrecv)
- CUBE triggers RTP and RTCP keepalive packets for the negotiated media streams.
- Supports only audio and video media types
- Supports media keepalive feature with High Availability (HA) deployments

Restrictions

The following are not supported with NAT media keepalive feature:

- Not supported for IPv6 destinations.
- Not supported for image or application m-lines.

Configure NAT Traversal using Media Keepalive

NAT traversal media keepalive configuration is applicable to the three configurations, listed here in order of preference:

- Dial-peer configuration
- Tenant configuration
- Global configuration

Configure NAT Media Keepalive at the Dial Peer Level

SUMMARY STEPS

1. **configure terminal**
2. **dial-peer voice *tag* voip**
3. **voice-class sip nat media-keepalive *interval***
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	dial-peer voice <i>tag</i> voip Example:	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

	Command or Action	Purpose
	Device(config)# <code>dial-peer voice 999 voip</code>	
Step 3	voice-class sip nat media-keepalive <i>interval</i> Example: Device(config-dial-peer)# <code>voice-class sip nat media-keepalive 40</code> Example: Device(config-dial-peer)# <code>voice-class sip nat media-keepalive</code>	Enables media keepalive allowing media keepalive packets to be transmitted for the specified interval of time (in seconds). Range is 1–50. Default value is 10. Note In the default configuration, no value is specified and keepalive interval is set to 10.
Step 4	exit Example: Device(config-dial-peer)# <code>exit</code>	Exits dial peer configuration mode and returns to global configuration mode.

Configure NAT Media Keepalive at the Tenant Level

SUMMARY STEPS

1. `configure terminal`
2. `voice class tenant tag`
3. `nat media-keepalive interval`
4. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	voice class tenant <i>tag</i> Example: Device(config)# <code>voice class tenant 1</code>	Associates a dial-peer with a specific tenant configuration.
Step 3	nat media-keepalive <i>interval</i> Example: Device(config-class)# <code>nat media-keepalive 35</code>	Enables media keepalive packets transmission for the specified interval of time (in seconds) at tenant level. Range is 1–50. Default value is 10.
Step 4	end Example: Device(config-dial-peer)# <code>end</code>	Returns to privileged EXEC mode.

Configure NAT Media Keepalive at the Global Level

SUMMARY STEPS

1. `configure terminal`
2. `voice service voip`
3. `sip`
4. `nat media-keepalive interval`
5. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>voice service voip</code> Example: Device(config)# <code>voice service voip</code>	Enters voice-service configuration mode and Voice over IP (VoIP) encapsulation type.
Step 3	<code>sip</code> Example: Device(config-voi-serv)# <code>sip</code>	Enters the Session Initiation Protocol (SIP) configuration mode.
Step 4	<code>nat media-keepalive interval</code> Example: Device(config-serv-sip)# <code>nat media-keepalive 20</code>	Enables media keepalive packets transmission for the specified interval of time (in seconds) at global level. Range is 1–50. Default value is 10.
Step 5	<code>end</code> Example: Device(config-serv-sip)# <code>end</code>	Returns to privileged EXEC mode.

Verify NAT Traversal using Media Keepalive Configuration

Use the following **show** commands to verify NAT media keepalive configurations at dial-peer level, tenant level, and global level configurations. You can enter the **show** commands in any order.

SUMMARY STEPS

1. `show run | sec dial-peer voice tag voip`
2. `show run | sec voice class tenant tag`
3. `show run | sec voice service voip`

4. show running-config all | sec media-keepalive

DETAILED STEPS

	Command or Action	Purpose
Step 1	show run sec dial-peer voice tag voip Example: <pre>Device# show run sec dial-peer voice 999 voip dial-peer voice 999 voip voice-class sip nat media-keepalive 40</pre>	The following sample output displays the NAT media keepalive for dial-peer configuration:
Step 2	show run sec voice class tenant tag Example: <pre>Device# show run sec voice class tenant 1 voice class tenant 1 nat media-keepalive 45</pre>	The following sample output displays the NAT media keepalive for tenant configuration:
Step 3	show run sec voice service voip Example: <pre>Device# show run sec voice service voip voice service voip sip nat media-keepalive 30</pre>	The following sample output displays NAT media keepalive for global configuration:
Step 4	show running-config all sec media-keepalive Example: <pre>Device# show running-config all sec media-keepalive nat media-keepalive 45 nat media-keepalive 30 voice-class sip nat media-keepalive 40</pre>	The following sample output displays the NAT media keepalive for all the configurations:

Configuration Example

Dial-peer level configuration

```
dial-peer voice 644 voip
session protocol sipv2
voice-class sip nat media-keepalive
codec g711ulaw
```

Global level configuration

```
voice service voip
sip
```

```
nat media-keepalive
```

Tenant level configuration

```
voice class tenant 1
  nat media-keepalive
  !
dial-peer voice 645 voip
  session protocol sipv2
  voice-class sip tenant 1
  codec g711ulaw
```




CHAPTER 50

Configure Report Generation

- [Overview, on page 467](#)
- [Prerequisites, on page 468](#)
- [Restrictions, on page 468](#)
- [Configure RTCP Report Generation, on page 468](#)
- [Troubleshooting Tips, on page 469](#)

Overview

The assisted Real-time Transport Control Protocol (RTCP) feature adds the ability for Cisco Unified Border Element (CUBE) to generate standard RTCP keepalive reports on behalf of endpoints. RTCP reports determine the liveliness of a media session during prolonged periods of silence, such as call hold or mute. Therefore, it is important for the CUBE to generate RTCP reports irrespective of whether the endpoints send or receive media.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information

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 71: Feature Information for Configuring RTCP Report Generation

Feature Name	Releases	Feature Information
Assisted RTCP	Baseline Functionality	The following commands were introduced or modified in this release: rtcp keepalive , debug voip rtcp , debug voip rtp , debug ip rtp protocol , and ip rtcp report interval .

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 15.1(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 3.17S or a later release must be installed and running on your Cisco ASR 1000 Series Router and Cisco ISR 4000 Series Router.

Restrictions

- RTCP report generation over IPv6 is not supported.
- RTCP report generation is not supported for Secure Real-time Transport Protocol (SRTP) or SRT Control Protocol (SRTCP) pass-through as CUBE is not aware of the media encryption or decryption keys.
- RTCP report generation is not supported for loopback calls, T.38 fax, and modem relay calls.
- RTCP or SRTCP report generation is not supported when CUBE inserts a Digital Signal Processor (DSP) for RTP-SRTP interworking on RTP and SRTP call legs.
- RTCP report generation is not supported when there is a call hold with an invalid media address such as 0.0.0.0 in Session Description Protocol (SDP) or Open Logical Channel (OLC).
- RTCP report generation is not supported for RTCP multiplexed with RTP on the same address and port.
- RTCP report generation is not supported on enterprise aggregation services routers (ASRs) and 4000 series integrated services routers (ISRs) when Media Termination Points are collocated with the CUBE. It affects RFC2833 and RFC4733 DTMF generation when MTP is used for DTMF conversion from Out-of-Band (OOB) to RFC2833 or RFC4733.

Configure RTCP Report Generation

RTCP keepalive packets indicate session liveliness. When configured on CUBE, RTCP keepalive packets are sent on both inbound and outbound SIP call legs.

Perform this task to configure RTCP report generation on CUBE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections** *from-type* **to** *to-type*
5. **rtcp keepalive**

6. 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 service voip Example: Router(config)# voice service voip	Enters voice service configuration mode.
Step 4	allow-connections <i>from-type</i> to <i>to-type</i> Example: Router(conf-voi-serv)# allow-connections sip to sip	Allows connections between SIP endpoints in a VoIP network.
Step 5	rtcp keepalive Example: Router(conf-voi-serv)# rtcp keepalive	Configures RTCP keepalive report generation.
Step 6	end Example: Router(conf-voi-serv)# end	Exits voice service configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the following debug commands for debugging related to RTCP keepalive packets:

- **debug voip rtcp packet** --Shows details related to RTCP keepalive packets such as RTCP sending and receiving paths, Call ID, Globally Unique Identifier (GUID), packet header, and so on.

```
Router# debug voip rtcp packet
01:06:27.450: //6/xxxxxxxxxxxx/RTP//Event/voip_rtp_send_rtcp_keepalive: Generate RTCP
Keepalive
*Mar 17 01:06:27.450: rtcp_send_report: Attributes
```

```

(src ip=192.168.30.3, src port=17101, dst ip=192.168.30.4, dst port=18619
 bye=0, initial=1, ssrc=0x07111E02, keepalive=1)
*Mar 17 01:06:27.450: rtcp_construct_keepalive_report: Constructed Report
(rtcp=0x2E5AF214, ssrc=0x07111E02, source->ssrc=0x00001E03, total_len=36)
2E5AF210:      80C90001 07111E02 81CA0006      .I.....J..
2E5AF220: 07111E02 010F302E 302E3040 392E3435      .....0.0.0@9.45
2E5AF230: 2E33302E 33000000 00              .30.3....

```



Caution Under moderate traffic loads, the **debug voip rtp packet** command produces a high volume of output and the command should be enabled only when the call volume is very low.

- **debug voip rtp packet** --Shows details about VoIP RTP packet debugging trace.

```

Router# debug voip rtp packet
VOIP RTP All Packets debugging is on

```

- **debug voip rtp session** --Shows all RTP session debug information.

```

Router# debug voip rtp session
VOIP RTP All Events debugging is on

```

- **debug voip rtp error** --Shows details about debugging trace for RTP packet error cases.

```

Router# debug voip rtp error
VOIP RTP Errors debugging is on

```

- **debug ip rtp protocol** --Shows details about RTP protocol debugging trace.

```

Router# debug ip rtp protocol
RTP protocol debugging is on

```

- **debug voip rtp session** --Shows all RTCP session debug information.

```

Router# debug voip rtcp session
VOIP RTCP Events debugging is on

```

- **debug voip rtcp error** -- Shows details about debugging trace for RTCP packet error cases.

```

Router# debug voip rtcp error
VOIP RTCP Errors debugging is on

```




PART **VIII**

Media Forking

- [Dial-peer Based Recording, on page 473](#)
- [SIP Forking, on page 499](#)
- [Video Recording, on page 531](#)
- [Third-Party GUID Capture, on page 537](#)
- [Network based Recording, on page 543](#)
- [Media Proxy and Recording, on page 559](#)
- [WebSocket-Based Media Forking for Cloud Speech Services, on page 591](#)



CHAPTER 51

Dial-peer Based Recording

- [Dial-peer Based Recording, on page 473](#)
- [Restrictions, on page 477](#)
- [Configure Dial-peer Recording, on page 478](#)
- [Additional References for Network-Based Recording, on page 498](#)

Dial-peer Based Recording

The Dial-peer Based Recording feature supports software-based forking for Real-time Transport Protocol (RTP) streams. Media forking provides the ability to create midcall multiple streams (or branches) of audio and video associated with a single call and then send the streams of data to different destinations. To enable network-based recording using Cisco Unified Border Element (CUBE), you can configure specific commands or use a call agent. CUBE acts as a recording client and MediaSense Session Initiation Protocol (SIP) recorder acts as a recording server.

Feature Information

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 72: Feature Information for Network-Based Recording

Feature Name	Releases	Feature Information
Security Readiness Criteria (SRC)—Modified the command show sip-ua calls .	Cisco IOS XE Gibraltar Release 16.11.1a	Command show sip-ua calls is modified to display local crypto key and remote crypto key.

Deployment Scenarios for CUBE-based Recording

CUBE as a recording client has the following functions:

- Acts as a SIP user agent and sets up a recording session (SIP dialog) with the recording server.

- Acts as the source of the recorded media and forwards the recorded media to the recording server.
- Sends information to a server that helps the recording server associate the call with media streams and identifies the participants of the call. This information sent to the recording server is called metadata.

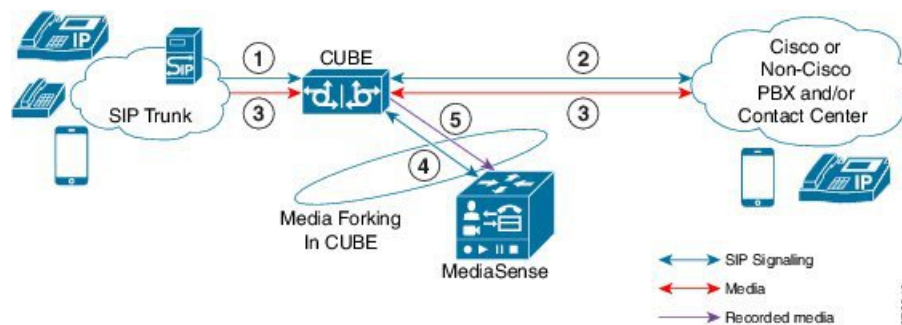


Note CUBE simply forwards the RTP streams it receives to the SIP recorder. It does not support omitting any pre-agent VRU activity from the recording.

If you want to omit the VRU segment from a recording, you must use the Unified CVP to route the agent segment of the call back through CUBE. To do this, you need to separate ingress and media forking function from one another, which means you must either route the call through the ingress router a second time, or route it through a second router.

Given below is a typical deployment scenario of a CUBE-based recording solution. The information flow is described below:

Figure 37: Deployment Scenario for CUBE-based Recording Solution



1. Incoming call from SIP trunk.
2. Outbound call to a Contact Centre
3. Media between endpoints flowthrough CUBE
4. CUBE sets up a new SIP session with MediaSense based on policy.
5. CUBE forks RTP media to MediaSense. For an audio call, audio is forked. For a video call, both audio and video are .forked. For an audio-only configuration in a audio-video call, only audio is forked. There will be two or four m-lines to the recording server, based on the type of recording

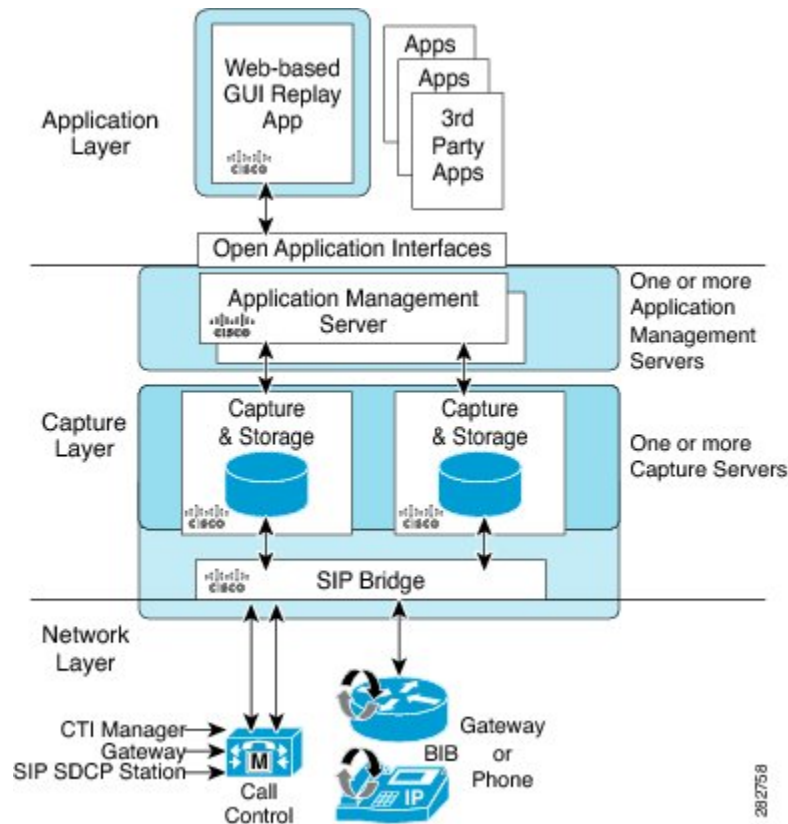
The metadata carried in the SIP session between the recording client and the recording server is to:

- Carry the communication session data that describes the call.
- Send the metadata to the recording server. The recording server uses the metadata to associate communication sessions involving two or more participants with media streams.

The call leg that is created between the recording client and the recording server is known as the recording session.

Open Recording Architecture

The Open Recording Architecture (ORA) comprises of elements, such as application management server and SIP bridge, to support IP-based recording. The ORA IP enables recording by solving topology issues, which accelerates the adoption of Cisco unified communication solutions.



Following are the three layers of the ORA architecture:

Network Layer

The ORA network layer is comprised of call control systems, media sources, and IP foundation components, such as routers and switches.

Capture and Media Processing Layer

The ORA capture and media processing layer includes core functions of ORA—terminating media streams, storage of media and metadata, and speech analytics that can provide real-time events for applications.

Application Layer

The ORA application layer supports in-call and post-call applications through open programming interfaces.

In-call applications include applications that make real-time business decisions (for example, whether to record a particular call or not), control pause and resume from Interactive Voice Response (IVR) or agent desktop systems, and perform metadata tagging and encryption key exchange at the call setup.

Post-call applications include the following:

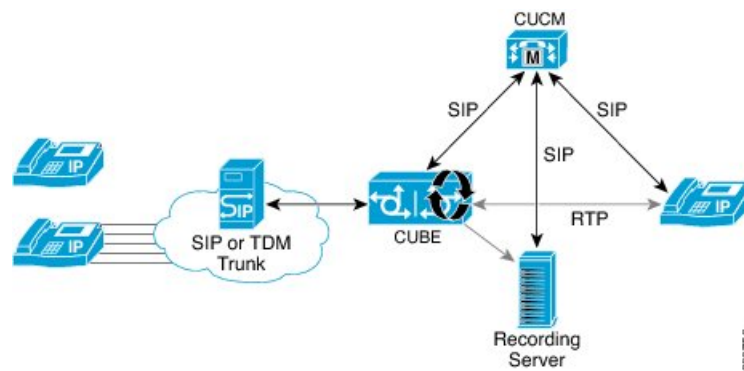
- Traditional compliance search, replay, and quality monitoring.
- Advanced capabilities, such as speech analytics, transcription, and phonetic search.
- Custom enterprise integration.
- Enterprise-wide policy management.

Media Forking Topologies

The following topologies support media forking:

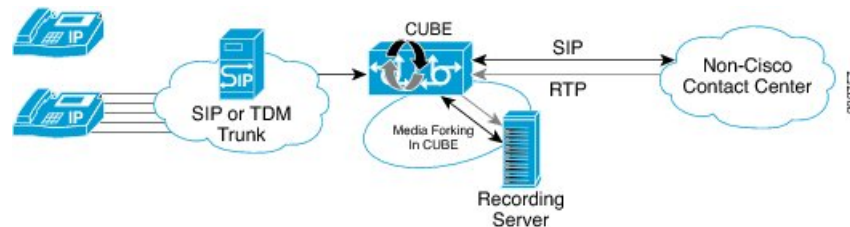
Media Forking with Cisco UCM

The figure below illustrates media forking with Cisco Unified CallManager (Cisco UCM) topology. This topology supports replication of media packets to allow recording by the caller agent. It also enables CUBE to establish full-duplex communication with the recording server. In this topology, SIP recording trunk is enhanced to have additional call metadata.



Media Forking without Cisco UCM

The topology below shows media forking without the Cisco UCM topology. This topology supports static configuration on CUBE and the replication of media packets to allow recording caller-agent and full-duplex interactions at an IP call recording server.



SIP Recorder Interface

SIP is used as a protocol between CUBE and the MediaSense SIP server. Extensions are made to SIP to carry the recording session information needed for the recording server. This information carried in SIP sessions between the recording client and the recording server is called metadata.

Metadata

Metadata is the information that is passed by the recording client to the recording server in a SIP session. Metadata describes the communication session and its media streams.

Metadata is used by the recording server to:

- Identify participants of the call.
- Associate media streams with the participant information. Each participant can have one or more media streams, such as audio and video.
- Identify the participant change due to transfers during the call.

The recording server uses the metadata information along with other SIP message information, such as dialog ID and time and date header, to derive a unique key. The recording server uses this key to store media streams and associate the participant information with the media streams.

Restrictions

- Dial-peer recording is not supported for the following calls:
 - Flow-around calls
 - Session Description Protocol (SDP) pass-through calls
 - Real-time Transport Protocol (RTP) loopback calls
 - High-density transcoder calls
 - IPv6-to-IPv6 calls
 - IPv6-to-IPv4 calls with IPv4 endpoint.
 - Secure Real-time Transport Protocol (SRTP) passthrough calls
 - SRTP-RTP calls with forking for SRTP leg (forking is supported for the RTP leg)
 - Resource Reservation Protocol (RSVP)
 - Multicast music on hold (MOH)
- Any media service parameter change via Re-INVITE or UPDATE from Recording server is not supported. Midcall renegotiation and supplementary services can be done through the primary call only.
- Recording is not supported if CUBE is running a TCL IVR application with the exception of survivability.tcl, which is supported with network based recording.
- Media mixing on forked streams is not supported

- Digital Signal Processing (DSP) resources are not supported on forked legs
- RecordTone insertion is not supported with SRTP calls.
- MediaForkingReason tag is to notify midcall stream events. Notification for codec change is not supported.
- Forking a single call on a CUBE using both dial-peer based recording and SIPREC is not supported.

Restrictions for Video Recording

- If the main call has multiple video streams (m-lines), the video streams other than the first video m-line are not forked.
- Application media streams of the primary call are not forked to the recording server.
- Forking is not supported if the anchor leg or recording server is on IPv6.
- High availability is not supported on forked video calls.
- Server Groups in outbound dial-peers towards recorders is not supported.

Configure Dial-peer Recording

Configure Dial-peer Recording (with Media Profile Recorder)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile recorder** *profile-tag*
4. (Optional) **media-type audio**
5. **media-recording** *dial-peer-tag* [*dial-peer-tag2...dial-peer-tag5*]
6. **exit**
7. **media class** *tag*
8. **recorder profile** *tag*
9. **exit**
10. **dial-peer voice** *dummy-recorder-dial-peer-tag* **voip**
11. **media-class** *tag*
12. **destination-pattern** **[+]** *string* **[T]**
13. **session protocol sipv2**
14. **session target ipv4:***[recording-server-destination-address | recording-server-dns]*
15. **session transport tcp**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile recorder <i>profile-tag</i> Example: Device(config)# media profile recorder 100	Configures the media profile recorder and enters media profile configuration mode.
Step 4	(Optional) media-type audio Example: Device(cfg-mediaprofile)# media-type audio	Configures recording of audio only in a call with both audio and video. If this configuration is not done, both audio and video are recorded.
Step 5	media-recording <i>dial-peer-tag</i> [<i>dial-peer-tag2...dial-peer-tag5</i>] Example: Device(cfg-mediaprofile)# media-recording 8000 8001 8002	Configures the dial-peers that need to be configured. Note You can specify a maximum of five dial-peer tags.
Step 6	exit Example: Device(cfg-mediaprofile)# exit	Exits media profile configuration mode.
Step 7	media class <i>tag</i> Example: Device(config)# media class 100	Configures a media class and enters media class configuration mode.
Step 8	recorder profile <i>tag</i> Example: Device(cfg-mediaclass)# recorder profile 100	Configures the media profile recorder.
Step 9	exit Example: Device(cfg-mediaclass)# exit	Exits media class configuration mode.

	Command or Action	Purpose
Step 10	dial-peer voice <i>dummy-recorder-dial-peer-tag</i> voip Example: Device(config)# dial-peer voice 8000 voip	Configures a recorder dial peer and enters dial peer voice configuration mode.
Step 11	media-class <i>tag</i> Example: Device(config-dial-peer)# media-class 100	Configures media class on a dial peer.
Step 12	destination-pattern [+] <i>string</i> [T] Example: Device(config-dial-peer)# destination-pattern 595959	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer. Note The predefined valid entries for <i>string</i> are the digits 0 to 9, the letters A to F and, the following special characters: <ul style="list-style-type: none"> • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Plus sign (+), which indicates that the preceding digit occurred one or more times. • Backslash symbol (\), which is followed by a single character, and matches that character. Media Forking functionality does not work with the wildcard entries other than the predefined set.
Step 13	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the VoIP dial peer to use Session Initiation Protocol (SIP).
Step 14	session target ipv4: <i>[recording-server-destination-address recording-server-dns]</i> Example: Device(config-dial-peer)# session target ipv4:10.42.29.7	Specifies a network-specific address for a dial peer. Keyword and argument are as follows: <ul style="list-style-type: none"> • ipv4: <i>destination address</i> --IP address of the dial peer, in this format: <i>xxx.xxx.xxx.xxx</i>
Step 15	session transport tcp Example: Device(config-dial-peer)# session transport tcp	Configures a VoIP dial peer to use Transmission Control Protocol (TCP).
Step 16	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-dial-peer)# end	

Configure Dial-peer Recording (without Media Profile Recorder)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media class tag**
4. **recorder parameter**
5. (Optional) **media-type audio**
6. **media-recording dial-peer-tag**
7. **exit**
8. **exit**
9. **dial-peer voice dummy-recorder-dial-peer-tag voip**
10. **media-class tag**
11. **destination-pattern [+] string [T]**
12. **session protocol sipv2**
13. **session target ipv4:[recording-server-destination-address | recording-server-dns]**
14. **session transport tcp**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media class tag Example: Device(config)# media class 100	Configures the media class and enters media class configuration mode.
Step 4	recorder parameter Example: Device(cfg-mediaclass)# recorder parameter	Enters media class recorder parameter configuration mode to enable you to configure recorder-specific parameters.

	Command or Action	Purpose
Step 5	(Optional) media-type audio Example: Device(cfg-mediaprofile)# media-type audio	Configures recording of audio only in a call with both audio and video. Note If this configuration is not done, both audio and video are recorded.
Step 6	media-recording dial-peer-tag Example: Device(cfg-mediaclass-recorder)# media-recording 8000, 8001, 8002	Configures voice-class recording parameters. Note You can specify a maximum of five dial-peer tags.
Step 7	exit Example: Device(cfg-mediaclass-recorder)# exit	Exits media class recorder parameter configuration mode.
Step 8	exit Example: Device(cfg-mediaclass)# exit	Exits media class configuration mode.
Step 9	dial-peer voice dummy-recorder-dial-peer-tag voip Example: Device(config)# dial-peer voice 8000 voip	Configures a recorder dial peer and enters dial peer voice configuration mode.
Step 10	media-class tag Example: Device(config-dial-peer)# media-class 100	Configures media class on a dial peer.
Step 11	destination-pattern [+] string [T] Example: Device(config-dial-peer)# destination-pattern 595959	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.

	Command or Action	Purpose
		<p>Note The predefined valid entries for <i>string</i> are the digits 0 to 9, the letters A to F and, the following special characters:</p> <ul style="list-style-type: none"> • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Plus sign (+), which indicates that the preceding digit occurred one or more times. • Backslash symbol (\), which is followed by a single character, and matches that character. <p>Media Forking functionality does not work with the wildcard entries other than the predefined set.</p>
Step 12	<p>session protocol sipv2</p> <p>Example:</p> <pre>Device(config-dial-peer)# session protocol sipv2</pre>	Configures the VoIP dial peer to use Session Initiation Protocol (SIP).
Step 13	<p>session target</p> <p>ipv4:<i>[recording-server-destination-address recording-server-dns]</i></p> <p>Example:</p> <pre>Device(config-dial-peer)# session target ipv4:10.42.29.7</pre>	<p>Specifies a network-specific address for a dial peer. Keyword and argument are as follows:</p> <ul style="list-style-type: none"> • ipv4: <i>destination address</i> --IP address of the dial peer, in this format: <i>xxx.xxx.xxx.xxx</i>
Step 14	<p>session transport tcp</p> <p>Example:</p> <pre>Device(config-dial-peer)# session transport tcp</pre>	Configures a VoIP dial peer to use Transmission Control Protocol (TCP).
Step 15	<p>end</p> <p>Example:</p> <pre>Device(config-dial-peer)# end</pre>	Returns to privileged EXEC mode.

Verifying the Dial-peer Recording

Perform this task to verify the configuration of the Network-Based Recording Using CUBE. The **show** and **debug** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show voip rtp connections**
3. **show voip recmsp session**

4. **show voip recmsp session detail call-id** *call-id*
5. **show voip rtp forking**
6. **show call active voice compact**
7. **show call active video compact**
8. **show sip-ua calls**
9. **show call active video brief**
10. **debug ccsip messages** (for audio calls)
11. **debug ccsip messages** (for video calls)
12. **debug ccsip messages** (for audio-only recording in a call with both audio and video)
13. Enter one of the following:
 - **debug ccsip all**
 - **debug voip recmsp all**
 - **debug voip ccapi all**
 - **debug voip fpi all** (for ASR devices only)

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show voip rtp connections**

Displays Real-Time Transport Protocol (RTP) connections. Two extra connections are displayed for forked legs.

Example:

```
Device# show voip rtp connections
```

```
VoIP RTP Port Usage Information:
```

```
Max Ports Available: 8091, Ports Reserved: 101, Ports in Use: 8
```

```
Port range not configured, Min: 16384, Max: 32767
```

Media-Address Range	Ports Available	Ports Reserved	Ports In-use
Default Address-Range	8091	101	8

VoIP RTP active connections :						
No.	CallId	dstCallId	LocalRTP	RmtRTP	LocalIP	RemoteIP
1	1	2	16384	20918	10.104.45.191	10.104.8.94
2	2	1	16386	17412	10.104.45.191	10.104.8.98
3	3	4	16388	29652	10.104.45.191	10.104.8.98
4	4	3	16390	20036	10.104.45.191	10.104.8.94
5	6	5	16392	58368	10.104.45.191	10.104.105.232

```

6      7          5          16394    53828  10.104.45.191          10.104.105.232
7      8          5          16396    39318  10.104.45.191          10.104.105.232
8      9          5          16398    41114  10.104.45.191          10.104.105.232

```

Found 8 active RTP connections

Step 3 **show voip recmsp session**

Displays active recording Media Service Provider (MSP) session information internal to CUBE.

Example:

```

Device# show voip recmsp session

RECMSP active sessions:
MSP Call-ID          AnchorLeg Call-ID      ForkedLeg Call-ID
143                  141                    145
Found 1 active sessions

```

Step 4 **show voip recmsp session detail call-id call-id**

Displays detailed information about the recording MSP Call ID.

Example:

```

Device# show voip recmsp session detail call-id 145
RECMSP active sessions:
Detailed Information
=====
Recording MSP Leg Details:
Call ID: 143
GUID : 7C5946D38ECD

AnchorLeg Details:
Call ID: 141
Forking Stream type: voice-nearend
Participant: 708090

Non-anchor Leg Details:
Call ID: 140
Forking Stream type: voice-farend
Participant: 10000

Forked Leg Details:
Call ID: 145
Near End Stream CallID 145
Stream State ACTIVE
Far End stream CallID 146
Stream State ACTIVE
Found 1 active sessions

Device# show voip recmsp session detail call-id 5

RECMSP active sessions:
Detailed Information
=====
Recording MSP Leg Details:
Call ID: 5
GUID : 1E01B6000000

AnchorLeg Details:
Call ID: 1

```

```

Forking Stream type: voice-nearend
Forking Stream type: video-nearend
Participant: 1777

```

```

Non-anchor Leg Details:
Call ID: 2
Forking Stream type: voice-farend
Forking Stream type: video-farend
Participant: 1888

```

```

Forked Leg Details:
Call ID: 6
Voice Near End Stream CallID 6
Stream State ACTIVE
Voice Far End stream CallID 7
Stream State ACTIVE
Video Near End stream CallID 8
Stream State ACTIVE
Video Far End stream CallID 9
Stream State ACTIVE
Found 1 active sessions

```

Output Field	Description
Stream State	Displays the state of the call. This can be ACTIVE or HOLD.
Msp Call-Id	Displays an internal Media service provider call ID and forking related statistics for an active forked call.
Anchor Leg Call-id	Displays an internal anchor leg ID, which is the dial peer where forking enabled. The output displays the participant number and stream type. Stream type voice-near end indicates the called party side.
Non-Anchor Call-id	Displays an internal non-anchor leg ID, which is the dial peer where forking is not enabled. The output displays the participant number and stream type. Stream type voice-near end indicates the called party side.
Forked Call-id	This forking leg call-id will show near-end and far-end stream call-id details with state of the Stream . Displays an internal foked leg ID. The output displays near-end and far-end details of a stream.

Step 5 show voip rtp forking

Displays RTP media-forking connections.

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 10.42.29.7, remote port 38526, local port 18648
    codec g711ulaw, logical ssrc 0x53
    packets sent 29687, packets received 0
  stream type voice+dtmf-nearend (4): count 0
  stream type voice-farend (5): count 1

```



```

remote ip 10.42.29.7, remote port 50482, local port 17780
  codec g711ulaw, logical ssrc 0x55
  packets sent 29686, packets received 0
stream type voice+dtmf-farend (6): count 0
stream type video (7): count

```

Output Field	Description
remote ip 10.42.29.7, remote port 38526, local port 18648	Recording server IP, recording server port, and local CUBE device port where data for stream 1 was first sent from.
remote ip 10.42.29.7, remote port 50482, local port 17780	Recording server IP, recording server port, and local CUBE device port where data for stream 2 was first sent from.
packets sent 29686	Number of packets sent to the recorder
codec g711ulaw	Codec negotiated for the recording leg.

Step 6 show call active voice compact

Displays a compact version of voice calls in progress. An additional call leg is displayed for media forking.

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
      140 ANS      T644   g711ulaw  VOIP      P10000           10.42.30.32:18638
      141 ORG      T644   g711ulaw  VOIP      P708090          10.42.30.189:26184
      145 ORG      T643   g711ulaw  VOIP      P595959          10.42.29.7:38526

```

Step 7 show call active video compact

Displays a compact version of 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: 3
      1 ANS      T14    H264      VOIP-VIDEO P1777           10.104.8.94:20036
      2 ORG      T14    H264      VOIP-VIDEO P1888           10.104.8.98:29652
      6 ORG      T13    H264      VOIP-VIDEO P1234           10.104.105.232:39318

```

Step 8 show sip-ua calls

Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls.

Example:

```

Device# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID      : C9A3AA00-B49A11E8-8018A74B-CD0B0450@10.0.0.1
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number    : 1234
Called Number     : 9876
Called URI        : sip:9876@10.0.0.2:9800
Bit Flags         : 0xC04018 0x90000100 0x80

```

```

CC Call ID           : 13
Local UUID          : 7d14e2d622ec504f9aaa4ba029ddd136
Remote UUID        : 2522eaa82f505c868037da95438fc49b
Source IP Address (Sig) : 10.0.0.1
Destn SIP Req Addr:Port : [10.0.0.2]:9800
Destn SIP Resp Addr:Port: [10.0.0.2]:9800
Destination Name    : 10.0.0.2
Number of Media Streams : 2
Number of Active Streams: 2
RTP Fork Object    : 0x0
Media Mode         : flow-through
Media Stream 1
  State of the stream : STREAM_ACTIVE
  Stream Call ID     : 13
  Stream Type        : voice-only (0)
  Stream Media Addr Type : 1
  Negotiated Codec   : g711ulaw (160 bytes)
  Codec Payload Type : 0
  Negotiated Dtmf-relay : inband-voice
  Dtmf-relay Payload Type : 0
  QoS ID             : -1
  Local QoS Strength : BestEffort
  Negotiated QoS Strength : BestEffort
  Negotiated QoS Direction : None
  Local QoS Status   : None
  Media Source IP Addr:Port: [10.0.0.1]:8022
  Media Dest IP Addr:Port : [10.0.0.2]:6008
  Local Crypto Suite : AES_CM_128_HMAC_SHA1_80 (
                        AEAD_AES_256_GCM
                        AEAD_AES_128_GCM
                        AES_CM_128_HMAC_SHA1_80
                        AES_CM_128_HMAC_SHA1_32 )
  Remote Crypto Suite : AES_CM_128_HMAC_SHA1_80
  Local Crypto Key    : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z1234tVb2
  Remote Crypto Key   : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z9876tVb2
Media Stream 2
  State of the stream : STREAM_ACTIVE
  Stream Call ID     : 14
  Stream Type        : video (7)
  Stream Media Addr Type : 1
  Negotiated Codec   : h264 (0 bytes)
  Codec Payload Type : 97
  Negotiated Dtmf-relay : inband-voice
  Dtmf-relay Payload Type : 0
  QoS ID             : -1
  Local QoS Strength : BestEffort
  Negotiated QoS Strength : BestEffort
  Negotiated QoS Direction : None
  Local QoS Status   : None
  Media Source IP Addr:Port: [10.0.0.1]:8020
  Media Dest IP Addr:Port : [10.0.0.2]:9802
  Local Crypto Suite : AES_CM_128_HMAC_SHA1_80 (
                        AEAD_AES_256_GCM
                        AEAD_AES_128_GCM
                        AES_CM_128_HMAC_SHA1_80
                        AES_CM_128_HMAC_SHA1_32 )
  Remote Crypto Suite : AES_CM_128_HMAC_SHA1_80
  Local Crypto Key    : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z2345tVb2
  Remote Crypto Key   : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z8765tVb2
Mid-Call Re-Association Count: 0
SRTP-RTP Re-Association DSP Query Count: 0

```

```
Options-Ping    ENABLED:NO    ACTIVE:NO
```

Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO

Call 1

```

SIP Call ID          : 1-12049@10.0.0.2
State of the call    : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number       : 1234
Called Number        : 9876
Called URI           : sip:9876@10.0.0.1:5060
Bit Flags            : 0xC0401C 0x10000100 0x4
CC Call ID          : 11
Local UUID           : 2522eaa82f505c868037da95438fc49b
Remote UUID          : 7d14e2d622ec504f9aaa4ba029ddd136
Source IP Address (Sig) : 10.0.0.1
Destn SIP Req Addr:Port : [10.0.0.2]:5060
Destn SIP Resp Addr:Port: [10.0.0.2]:5060
Destination Name     : 10.0.0.2
Number of Media Streams : 2
Number of Active Streams: 2
RTP Fork Object      : 0x0
Media Mode           : flow-through

Media Stream 1
State of the stream   : STREAM_ACTIVE
Stream Call ID        : 11
Stream Type           : voice-only (0)
Stream Media Addr Type : 1
Negotiated Codec      : g711ulaw (160 bytes)
Codec Payload Type    : 0
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID                : -1
Local QoS Strength    : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status      : None
Media Source IP Addr:Port: [10.0.0.1]:8016
Media Dest IP Addr:Port : [10.0.0.2]:6009
Local Crypto Suite    : AES_CM_128_HMAC_SHA1_80
Remote Crypto Suite   : AES_CM_128_HMAC_SHA1_80
Local Crypto Key      : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z9876tVb2
Remote Crypto Key     : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z1234tVb2

Media Stream 2
State of the stream   : STREAM_ACTIVE
Stream Call ID        : 12
Stream Type           : video (7)
Stream Media Addr Type : 1
Negotiated Codec      : h264 (0 bytes)
Codec Payload Type    : 97
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID                : -1
Local QoS Strength    : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status      : None
Media Source IP Addr:Port: [10.0.0.1]:8018
Media Dest IP Addr:Port : [10.0.0.2]:5062
Local Crypto Suite    : AES_CM_128_HMAC_SHA1_80
Remote Crypto Suite   : AES_CM_128_HMAC_SHA1_80
Local Crypto Key      : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z8765tVb2
Remote Crypto Key     : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z2345tVb2

Mid-Call Re-Association Count: 0
SRTP-RTP Re-Association DSP Query Count: 0

```

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

Step 9 **show call active video brief**

Displays a truncated version of video calls in progress.

Example:

```
Device# show call active video brief
```

```
Telephony call-legs: 0
SIP call-legs: 3
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 3

0    : 1 87424920ms.1 (*12:23:53.573 IST Wed Jul 17 2013) +1050 pid:1 Answer 1777 active
  dur 00:00:46 tx:5250/1857831 rx:5293/1930598 dscp:0 media:0 audio tos:0xB8 video tos:0x88
  IP 10.104.8.94:20036 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms H264 TextRelay: off
Transcoded: No
...
0    : 2 87424930ms.1 (*12:23:53.583 IST Wed Jul 17 2013) +1040 pid:2 Originate 1888 active
  dur 00:00:46 tx:5293/1930598 rx:5250/1857831 dscp:0 media:0 audio tos:0xB8 video tos:0x88
  IP 10.104.8.98:29652 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms H264 TextRelay: off
Transcoded: No
...
0    : 6 87425990ms.1 (*12:23:54.643 IST Wed Jul 17 2013) +680 pid:1234 Originate 1234 active
  dur 00:00:46 tx:10398/3732871 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
  IP 10.104.105.232:39318 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms H264 TextRelay: off
Transcoded: No
...
```

Step 10 **debug ccsip messages (for audio calls)**

```
Sent:
INVITE sip:22222@10.42.29.7:5060 SIP/2.0
Via: SIP/2.0/TCP 10.42.30.10:5060;branch=z9hG4bKB622CF
X-Cisco-Recording-Participant: sip:708090@10.42.30.5;media-index="0"
X-Cisco-Recording-Participant: sip:10000@10.42.30.32;media-index="1"
From: <sip:10.42.30.10>;tag=5096700-1E1A
To: <sip:595959@10.42.29.7>
Date: Fri, 18 Mar 2011 07:01:50 GMT
Call-ID: 6E6CF813-506411E0-80EAE01B-4C27AA62@10.42.30.10
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE: 1800
Cisco-Guid: 1334370502-1348997600-2396699092-3395863316
User-Agent: Cisco-SIPGateway/IOS-15.2(0.0.2)PIA16
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1300431710
Contact: <sip:10.42.30.10:5060;transport=tcp>
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 449
v=0
o=CiscoSystemsSIP-GW-UserAgent 3021 3526 IN IP4 10.42.30.10
```

```

s=SIP Call
c=IN IP4 10.42.30.10
t=0 0
m=audio 24544 RTP/AVP 0 101 19
c=IN IP4 10.42.30.10
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
a=ptime:20
a=sendonly
m=audio 31166 RTP/AVP 0 101 19
c=IN IP4 10.42.30.10
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
a=ptime:20
a=sendonly
Received:
SIP/2.0 200 Ok
Via: SIP/2.0/TCP 10.104.46.198:5060;branch=z9hG4bK13262B
To: <sip:23232323@10.104.46.201>;tag=ds457251f
From: <sip:10.104.46.198>;tag=110B66-1CBC
Call-ID: 7142FB-9A5011E0-801EF71A-59B4D258@10.104.46.198
CSeq: 101 INVITE
Content-Length: 206
Contact: <sip:23232323@10.104.46.201:5060;transport=tcp>
Content-Type: application/sdp
Allow: INVITE, BYE, CANCEL, ACK, NOTIFY, INFO, UPDATE
Server: Cisco-ORA/8.5
v=0
o=CiscoORA 2187 1 IN IP4 10.104.46.201
s=SIP Call
c=IN IP4 10.104.46.201
t=0 0
m=audio 54100 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=recvonly
m=audio 39674 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=recvonly

Sent:
ACK sip:23232323@10.104.46.201:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 10.104.46.198:5060;branch=z9hG4bK141B87
From: <sip:10.104.46.198>;tag=110B66-1CBC
To: <sip:23232323@10.104.46.201>;tag=ds457251f
Date: Mon, 20 Jun 2011 08:42:01 GMT
Call-ID: 7142FB-9A5011E0-801EF71A-59B4D258@10.104.46.198
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

```

Output Field	Description
INVITE sip:22222@10.42.29.7:5060 SIP/2.0	22222 is the destination pattern or the number of recording server and is configured under the recorder dial peer.

Output Field	Description
X-Cisco-Recording-Participant: sip:708090@10.42.30.5;media-index="0"	Cisco proprietary header with originating and terminating participant number and IP address used to communicate to the recording server
Cisco-Guid: 1334370502-1348997600-2396699092-3395863316	GUID is the same for the primary call and forked call .
m=audio 24544 RTP/AVP 0 101 19	First m-line of participant with payload type and codec information .
m=audio 31166 RTP/AVP 0 101 19	Second m- line of another participant with codec info and payload type.
a=sendonly	CUBE is always in send only mode towards Recording server.
a=recvnly	Recording server is in receive mode only.

Step 11 debug ccsip messages (for video calls)

```

Sent: INVITE sip:575757@9.45.38.39:7686 SIP/2.0
.
.
Via: SIP/2.0/UDP 9.41.36.41:5060;branch=z9hG4bK2CC2408
X-Cisco-Recording-Participant: sip:1777@10.104.45.207;media-
index="0 2"
X-Cisco-Recording-Participant: sip:1888@10.104.45.207;media-   index="1 3"
.
.
Cisco-Guid: 0884935168-0000065536-0000000401-3475859466
.
.
v=0
.
.
.
m=audio 17232 RTP/AVP 0 19
.
.
a=sendonly
m=audio 17234 RTP/AVP 0 19
.
.
a=sendonly

m=video 17236 RTP/AVP 126
.
.
.

a=fmtp:126 profile-level-id=42801E;packetization-mode=1
a=sendonly
m=video 17238 RTP/AVP 126
.

```

```
.
.
a=fmtp:126 profile-level-id=42801E;packetization-mode=1
a=sendonly
```

Output Field	Description
Sent: INVITE sip:575757@9.45.38.39:7686 SIP/2.0	22222 is the destination pattern or the number of recording server and is configured under the recorder dial peer.
X-Cisco-Recording-Participant: sip:1777@10.104.45.207;media-index="0 2" X-Cisco-Recording-Participant: sip:1888@10.104.45.207;media-index="1 3"	Cisco proprietary header with originating and terminating participant number and IP address used to communicate to the recording server
Cisco-Guid: 0884935168-0000065536-0000000401-3475859466	GUID is the same for the primary call and forked call .
m=audio 17232 RTP/AVP 0 19	First m-line of participant with payload type and audio codec.
m=audio 17234 RTP/AVP 0 19	Second m-line of another participant with payload type and audio codec.
m=video 17236 RTP/AVP 126	Third m-line of participant with video payload type and codec info .
m=video 17238 RTP/AVP 126	Fourth m-line of another participant with video payload type and codec info .
a=sendonly	CUBE is always in send only mode towards Recording server.

```
Receive:
SIP/2.0 200 OK
.
.
.
v=0
.
.
m=audio 1592 RTP/AVP 0
.
.
a=recvonly
m=audio 1594 RTP/AVP 0
.
.
a=recvonly
m=video 1596 RTP/AVP 126
.
.
a=fmtp:97 profile-level-id=420015
a=recvonly
m=video 1598 RTP/AVP 126
.
.
a=fmtp:126 profile-level-id=420015
a=recvonly
```

```

Sent:
ACK sip:9.45.38.39:7686;transport=UDP SIP/2.0

Via: SIP/2.0/UDP 9.41.36.41:5060;branch=z9hG4bK2CD7

From: <sip:9.41.36.41>;tag=1ECFD128-24DF

To: <sip:575757@9.45.38.39>;tag=16104SIPpTag011

Date: Tue, 19 Mar 2013 11:40:01 GMT

Call-ID: FFFFFFFF91E00FE6-FFFFFFF8FC011E2-FFFFFFF824DF469-FFFFFFFB6661C06@9.41.36.41

Max-Forwards: 70

CSeq: 101 ACK

Allow-Events: telephone-event

Content-Length: 0

```

Output Field	Description
m=audio 1592 RTP/AVP 0	First m-line of recording server after it started listening.
m=audio 1594 RTP/AVP 0	Second m-line of recording server after it started listening.
m=video 1596 RTP/AVP 126	Third m-line of recording server after it started listening.
m=video 1598 RTP/AVP 126	Fourth m-line of recording server after it started listening.
a=recvonly	Recording server in receive only mode.

Step 12 debug ccsip messages (for audio-only recording in a call with both audio and video)

Displays offer sent to MediaSense having only audio m-lines, when the **media-type audio** command is configured.

```

Sent:
INVITE sip:54321@9.45.38.39:36212 SIP/2.0
Via: SIP/2.0/UDP 9.41.36.15:5060;branch=z9hG4bK2216B
X-Cisco-Recording-Participant: sip:4321@9.45.38.39;media-index="0"
X-Cisco-Recording-Participant: sip:1111000010@9.45.38.39;media-index="1"
From: <sip:9.41.36.15>;tag=A2C74-5D9
To: <sip:54321@9.45.38.39>.....
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 337

v=0
o=CiscoSystemsSIP-GW-UserAgent 9849 5909 IN IP4 9.41.36.15
s=SIP Call
c=IN IP4 9.41.36.15
t=0 0
m=audio 16392 RTP/AVP 0 19
c=IN IP4 9.41.36.15
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20
a=sendonly
m=audio 16394 RTP/AVP 0 19

```



```
c=IN IP4 9.41.36.15
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20
a=sendonly
```

Response from CUBE has inactive video m-lines.

```
Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.41.36.15:5060;branch=z9hG4bK2216B
...
v=0
...
m=audio 36600 RTP/AVP 0
c=IN IP4 9.45.38.39
a=rtpmap:0 PCMU/8000
a=ptime:20
a=recvonly
m=audio 36602 RTP/AVP 0
c=IN IP4 9.45.38.39
a=rtpmap:0 PCMU/8000
a=ptime:20
a=recvonly
m=video 0 RTP/AVP 98
c=IN IP4 9.45.38.39
b=TIAS:1500000
a=rtpmap:98 H264/90000
a=fmtp:98 profile-level-id=420015
a=inactive
m=video 0 RTP/AVP 98
c=IN IP4 9.45.38.39
b=TIAS:1500000
a=rtpmap:98 H264/90000
a=fmtp:98 profile-level-id=420015
a=inactive
```

Step 13

Enter one of the following:

- **debug ccsip all**
- **debug voip recmsp all**
- **debug voip ccapi all**
- **debug voip fpi all** (for ASR devices only)

Displays detailed debug messages.

For Audio:

Media forking initialized:

```
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_trigger_media_forking: MF: Recv Ack..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_trigger_media_forking: MF: Recv Ack & it's
Anchor leg. Start MF.
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_preprocess_event: MF:
initial-call. State = 1 & posting the event E_IPIP_MEDIA_FORKING_CALLSETUP_IND
```

Media forking started:

```
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_service_get_event_data: Event
id = 30
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Function/sipSPIUisValidCcb:
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Function/ccsip_is_valid_ccb:
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking: MF: Current State = 1,
event =30
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking: MF: State & Event
```

```

combination is cracked..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Function/sipSPIGetMainStream:
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Function/sipSPIGetMainStream:
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_precondition: MF: Can
be started with current config.
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecParticipant:
MF: Populate rec parti header from this leg.

```

Forking header populated:

```

*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF: X-Cisco
header is RPID..

```

Media forking setup record session is successful:

```

*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF:
Building SIP URL..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF: Sipuser
= 98459845
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF: Host
= 9.42.30.34
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Function/sipSPIGetFirstStream:
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Function/voip_media_dir_to_cc_media_dir:
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecStream: MF:
direction type =3 3
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecStream: MF:
callid 103 set to nearend..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecStream: MF:
dtmf is inband
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecStream: MF:
First element..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecParticipant:
MF: First element..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_BuildMediaRecParticipant:
MF: Populate rec parti header from peer leg.
*Jun 15 10:37:55.404: //104/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF: X-Cisco
header is RPID..
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_write_to_TDContainer:
MF: Data written to TD Container..
*Jun 15 10:37:55.404: //-1/xxxxxxxxxxxx/Event/recmsp_api_setup_session: Event: E_REC_SETUP_REQ
anchor call ID:103, msp call ID:105 infuncion recmsp_api_setup_session
*Jun 15 10:37:55.404: //-1/xxxxxxxxxxxx/Inout/recmsp_api_setup_session: Exit with Success
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/act_sip_mf_idle_callsetup_ind: MF:
setup_record_session is success..

```

Media forking forked stream started:

```

*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/sipSPIMFChangeState: MF: Prev state = 1 & New
state = 2
*Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_gen_service_process_event: MF: 30 event
handled.
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_call_setup_request: Set Protocol information
*Jun 15 10:37:55.406: //106/xxxxxxxxxxxx/CCAPI/cc_set_post_tagdata:
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_ipip_media_forking_read_from_TDContainer:
MF: Data read from TD container..
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_ipip_media_forking_forked_leg_config: MF:
MSP callid = 105
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_ipip_media_forking_forked_leg_config: MF:
Overwriting the GUID with the value got from MSP.
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_iwf_handle_peer_event:
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_iwf_map_ccapi_event_to_iwf_event: Event
Category: 1, Event Id: 179
*Jun 15 10:37:55.406: //106/000000000000/SIP/Info/ccsip_iwf_process_event:
*Jun 15 10:37:55.406: //106/000000000000/SIP/Function/sipSPIUisValidCcb:
*Jun 15 10:37:55.406: //106/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_add_forking_stream: MF:
Forked stream added..

```

```
*Jun 15 10:37:55.406: //106/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_read_from_TDContainer:
MF: Data read from TD container..
*Jun 15 10:37:55.406: //106/3E7E90AE8006/SIP/Function/sipSPIGetFirstStream:
*Jun 15 10:37:55.406: //106/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_Display_TDContainerData:
  ** DISPLAY REC PART **
*Jun 15 10:37:55.406: //106/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_Display_TDContainerData:
  recorder tag = 5
```

For Video:**Media Forking Initialized:**

```
*Mar 19 16:40:01.784 IST: //522/34BF0A000000/SIP/Info/notify/32768/ccsip_trigger_media_forking: MF:
  Recv Ack & it's Anchor leg. Start MF.
*Mar 19 16:40:01.784 IST:
//522/34BF0A000000/SIP/Info/info/32768/ccsip_ipip_media_forking_preprocess_event: MF: initial-call.
  State = 1 & posting the event E_IPIP_MEDIA_FORKING_CALLSETUP_IND
```

Media forking started:

```
*Mar 19 16:40:01.784 IST: //522/34BF0A000000/SIP/Info/info/36864/ccsip_ipip_media_forking: MF:
Current State = 1, event =31
*Mar 19 16:40:01.784 IST: //522/34BF0A000000/SIP/Info/info/36864/ccsip_ipip_media_forking: MF: State
  & Event combination is cracked..
*Mar 19 16:40:01.784 IST: //522/34BF0A000000/SIP/Function/sipSPIGetMainStream:
*Mar 19 16:40:01.784 IST: //522/34BF0A000000/SIP/Function/sipSPIGetMainStream:
*Mar 19 16:40:01.787 IST:
//522/34BF0A000000/SIP/Info/info/34816/ccsip_ipip_media_forking_precondition: MF: Can be started
  with current config.
*Mar 19 16:40:01.787 IST: //-1/xxxxxxxxxxxxx/Event/recmsp_api_create_session: Event:
E_REC_CREATE_SESSION anchor call ID:522, msp call ID:526
*Mar 19 16:40:01.787 IST: //-1/xxxxxxxxxxxxx/Inout/recmsp_api_create_session: Exit with Success
```

Recording participant for anchor leg:

```
//522/34BF0A000000/SIP/Info/verbose/32768/ccsip_ipip_media_forking_BuildMediaRecParticipant: MF:
Populate rec parti header from this leg.
*Mar 19 16:40:01.788 IST:
//522/34BF0A000000/SIP/Info/info/33792/ccsip_get_recording_participant_header: MF: X-Cisco header
  is PAI..
```

Adding an audio stream:

```
*Mar 19 16:40:01.788 IST: //522/34BF0A000000/SIP/Function/sipSPIGetFirstStream:
*Mar 19 16:40:01.788 IST:
//522/34BF0A000000/SIP/Info/verbose/32768/ccsip_ipip_media_forking_BuildMediaRecStream: MF: Adding
  a Audio stream..
*Mar 19 16:40:01.789 IST: //522/34BF0A000000/SIP/Function/voip_media_dir_to_cc_media_dir:
*Mar 19 16:40:01.789 IST:
//522/34BF0A000000/SIP/Info/info/32768/ccsip_ipip_media_forking_BuildAudioRecStream: MF: direction
  type =3 3
*Mar 19 16:40:01.789 IST:
//522/34BF0A000000/SIP/Info/info/32768/ccsip_ipip_media_forking_BuildAudioRecStream: MF: callid 522
  set to nearend..
*Mar 19 16:40:01.789 IST:
//522/34BF0A000000/SIP/Info/info/32768/ccsip_ipip_media_forking_BuildAudioRecStream: MF: This
  rcstream has 522 callid
*Mar 19 16:40:01.789 IST:
//522/34BF0A000000/SIP/Info/verbose/32768/ccsip_ipip_media_forking_BuildAudioRecStream: MF: Setting
  data for audio stream..
*Mar 19 16:40:01.789 IST:
//522/34BF0A000000/SIP/Info/info/32800/ccsip_ipip_media_forking_BuildAudioRecStream: MF: dtmf is
  inband
.
```

Video forking:

```
*Mar 19 16:40:01.789 IST: //522/34BF0A000000/SIP/Function/sipSPIGetVideoStream:
*Mar 19 16:40:01.789 IST:
//522/34BF0A000000/SIP/Info/verbose/32772/ccsip_ipip_media_forking_BuildMediaRecStream: MF:
video_codec_present,Continue with Video Forking..
```

For Video

Additional References for Network-Based Recording

Related Documents

MediaSense Installation and Administration Guide	Cisco MediaSense Installation and Administration Guide
--	--

Standards and RFCs

RFCs	Title
RFC 3984	<i>RTP Payload Format for H.264 Video</i>
RFC 5104	<i>Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)</i>
RFC 5168	<i>XML Schema for Media Control</i>



CHAPTER 52

SIP Forking

- [Overview, on page 499](#)
- [Prerequisites for SIPREC Recording, on page 501](#)
- [Restrictions for SIPREC Recording, on page 501](#)
- [Configure SIPREC-Based Recording, on page 502](#)
- [Configuration Examples for SIPREC-based Recording, on page 507](#)
- [Configuration Example for Metadata Variations with Different Mid-call Flows, on page 514](#)
- [Configuration Example for Metadata Variations with Different Transfer Flows, on page 526](#)
- [Configuration Examples for Metadata Variations with Caller-ID UPDATE Flow, on page 527](#)
- [Configuration Example for Metadata Variations with Call Disconnect, on page 528](#)

Overview

The SIPREC (SIP Forking) feature supports media recording for Real-time Transport Protocol (RTP) streams in compliance with section 3.1.1. of RFC 7245, with Cisco Unified Border Element (CUBE) acting as the Session Recording Client. SIP is used as a protocol between CUBE and the recording server. Recording of a media session is done by sending a copy of a media stream to the recording server. Metadata is the information that is passed by the recording client to the recording server in a SIP session. The recording metadata describes the communication session and its media streams, and also identifies the participants of the call. CUBE acts as the recording client and any third party recorder acts as the recording server.

Feature Information

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 73: Feature Information

Feature Name	Releases	Feature Information
SIPREC (SIP Recording)	Baseline Functionality	The following commands were modified: recorder parameter and recorder profile .

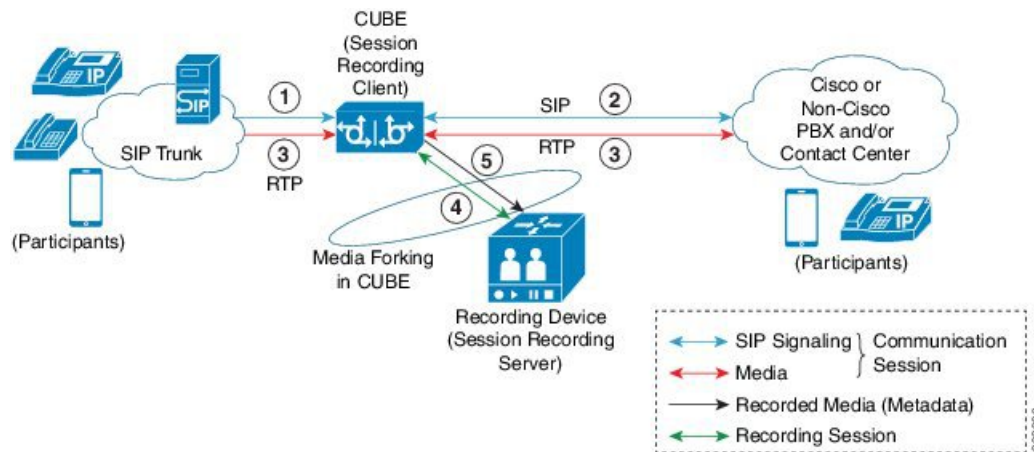
Deployment

You need to have:

- Participants — SIP UAs involved in the Communication Session. The UA can be any SIP element.
- Communication Session (CS) — Session established between the endpoints.
- Session Recording Client (SRC) — CUBE acts as the session recording client that triggers the recording session.
- Session Recording Server (SRS) — A SIP User Agent (UA) which is a specialized media server and that acts as a sink for the recorded media and metadata.
- Recording Session (RS) — SIP dialog established between CUBE (recording client) and the recording server.
- Recording Metadata — Information on the CS and the associated media stream data sent from CUBE to RS.

The following figure illustrates a third party recorder deployment with CUBE.

Figure 38: Deployment Scenario for SIPREC Recording Solution



Information flow is described below:

1. Incoming call from SIP trunk
2. Outbound call to Contact Center
3. Media between endpoints flowthrough CUBE
4. CUBE sets up a new SIP session with the recording device (SRS)
5. CUBE forks RTP media to SRS

In the preceding illustration, the Real Time Protocol (RTP) carries voice data and media streams between the user agents and CUBE. The RTP unidirectional stream represent the communication session forked from CUBE to the recording server to indicate forked media. The Session Initiation protocol (SIP) carries call signaling information along with the metadata information. Media streams from CUBE to recording server

are unidirectional because only CUBE sends recorded data to recording server; the recording server does not send any media to CUBE.

Metadata has the following functions:

- Carry the communication session data (audio and video calls) that describes the call to the recording server.
- Identifies the participants list.
- Identifies the session and media association time.

If there are any changes in the call sessions, for example, hold-resume, transfer and so on, these sessions are notified to the recording server through metadata.

Prerequisites for SIPREC Recording

Make sure that:

- Recorders must be reachable from CUBE
- SIPREC should be configured; else, CUBE will fall back to the existing Network-Based Recording implementation. For more information, see *Network-Based Recording* section.
- CUBE supports the SIP Recording Metadata model format requirements specified in [draft-ietf-siprec-metadata-17](#). Recorders must support metadata format of ver17 at a minimum
- CUBE should be in compliance with the Session Recording Protocols defined in [draft-ietf-siprec-protocol-16](#). CUBE supports only the “siprec Option” Tag and the “src feature” tag among the various other extensions defined in the protocols draft; CUBE does not support the SDP extensions.

Restrictions for SIPREC Recording

SIPREC-based recording is not supported for the following calls:

- Any media service parameter change via Re-INVITE or UPDATE from recording server is not supported. For example, hold-resume or any codec changes
- IPv6-to-IPv6 call recording
- IPv6-to-IPv4 call recording if the recording server is configured on the IPv6 call leg
- Flow-around calls
- Session Description Protocol (SDP) pass-through calls
- Real-time Transport Protocol (RTP) loopback calls
- High-density transcoder calls
- Secure Real-time Transport Protocol (SRTP) passthrough calls
- SRTP-RTP calls with forking for SRTP leg (forking is supported for the RTP leg)

- Multicast music on hold (MOH)
- Mid-call renegotiation and supplementary services like Hold/Resume, control pause, and so on are not supported on the recorder call leg
- Recording is not supported if CUBE is running a TCL IVR application with the exception of `survivability.tcl`, which is supported with SIPREC based recording
- Media mixing on forked streams is not supported
- Digital Signal Processing (DSP) resources are not supported on forked legs
- Forking a single call on a CUBE using both dial-peer based recording and SIPREC is not supported.

Restrictions for Video Recording

- If the main call has multiple video streams (m-lines), the video streams other than the first video m-line are not forked
- Application media streams of the primary call are not forked to the recording server
- Forking is not supported if the anchor leg or recording server is on IPv6
- Server Groups in outbound dial-peers towards recorders is not supported.

Configure SIPREC-Based Recording

Configure SIPREC-Based Recording (with Media Profile Recorder)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile recorder** *profile-tag*
4. (Optional) **media-type audio**
5. **media-recording** *dial-peer-tag* [*dial-peer-tag2...dial-peer-tag5*]
6. **exit**
7. **media class** *tag*
8. **recorder profile** *profile-tag siprec*
9. **exit**
10. **dial-peer voice** *dp-tag voip*
11. **session protocol sipv2**
12. **media-class** *tag*
13. **dial-peer voice** *dial-peer-tag voip*
14. **destination-pattern** **[+]** *string* **[T]**
15. **session protocol sipv2**
16. **session target ipv4:***[recording-server-destination-address | recording-server-dns]*
17. **session transport tcp**
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile recorder <i>profile-tag</i> Example: Device(config)# media profile recorder 100	Configures the media profile recorder and enters media profile configuration mode.
Step 4	(Optional) media-type audio Example: Device(cfg-mediaprofile)# media-type audio	Configures recording of audio only in a call with both audio and video. If this configuration is not done, both audio and video are recorded.
Step 5	media-recording <i>dial-peer-tag</i> [<i>dial-peer-tag2...dial-peer-tag5</i>] Example: Device(cfg-mediaprofile)# media-recording 8000 8001 8002	Configures the dial-peers that need to be configured Note You can specify a maximum of five dial-peer tags.
Step 6	exit Example: Device(cfg-mediaprofile)# exit	Exits media profile configuration mode.
Step 7	media class <i>tag</i> Example: Device(config)# media class 100	Configures a media class and enters media class configuration mode.
Step 8	recorder profile <i>profile-tag siprec</i> Example: Device(cfg-mediaclass)# recorder profile 201 siprec	Configures the media profile SIPREC recorder.
Step 9	exit Example:	Exits media class configuration mode.

	Command or Action	Purpose
	Device(cfg-mediaclass)# exit	
Step 10	dial-peer voice <i>dp-tag</i> voip Example: Device(config)# dial-peer voice 8000 voip	Configures a recorder dial peer and enters dial peer voice configuration mode.
Step 11	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the VoIP dial peer to use Session Initiation Protocol (SIP).
Step 12	media-class <i>tag</i> Example: Device(config-dial-peer)# media-class 100	Configures media class on a dial peer.
Step 13	dial-peer voice <i>dial-peer-tag</i> voip Example: Device(config)# dial-peer voice 8000 voip	Configures a recorder dial peer and enters dial-peer voice configuration mode.
Step 14	destination-pattern [+] <i>string</i> [T] Example: Device(config-dial-peer)# destination-pattern 595959	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
Step 15	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the VoIP dial peer to use Session Initiation Protocol (SIP).
Step 16	session target ipv4: <i>[recording-server-destination-address recording-server-dns]</i> Example: Device(config-dial-peer)# session target ipv4:10.42.29.7	Specifies a network-specific address for a dial peer. Keyword and argument are as follows: <ul style="list-style-type: none"> • ipv4: <i>destination address</i> --IP address of the dial peer, in this format: <i>xxx.xxx.xxx.xxx</i>
Step 17	session transport tcp Example: Device(config-dial-peer)# session transport tcp	Configures a VoIP dial peer to use Transmission Control Protocol (TCP).
Step 18	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-dial-peer)# end	

Configure SIPREC-Based Recording (without Media Profile Recorder)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media class tag**
4. **recorder parametersiprec**
5. (Optional) **media-type audio**
6. **media-recording dial-peer-tag**
7. **exit**
8. **exit**
9. **dial-peer voice dp-tag voip**
10. **session protocol sipv2**
11. **media-class tag**
12. **dial-peer voice dial-peer-tag voip**
13. **destination-pattern [+]** string [T]
14. **session protocol sipv2**
15. **session target ipv4:**[recording-server-destination-address | recording-server-dns]
16. **session transport tcp**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media class tag Example: Device(config)# media class 100	Configures the media class and enters media class configuration mode.

	Command or Action	Purpose
Step 4	recorder parametersiprec Example: Device(cfg-mediaclass)# recorder parameter siprec	Enables SIPREC recording.
Step 5	(Optional) media-type audio Example: Device(cfg-mediaprofile)# media-type audio	Configures recording of audio only in a call with both audio and video. Note If this configuration is not done, both audio and video are recorded.
Step 6	media-recording dial-peer-tag Example: Device(cfg-mediaclass-recorder)# media-recording 8000, 8001, 8002	Configures voice-class recording parameters. Note You can specify a maximum of five dial-peer tags.
Step 7	exit Example: Device(cfg-mediaclass-recorder)# exit	Exits media class recorder parameter configuration mode.
Step 8	exit Example: Device(cfg-mediaclass)# exit	Exits media class configuration mode.
Step 9	dial-peer voice dp-tag voip Example: Device(config)# dial-peer voice 1 voip	Dial peer that needs to be forked.
Step 10	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the VoIP dial peer to use Session Initiation Protocol (SIP).
Step 11	media-class tag Example: Device(config-dial-peer)# media-class 100	Configures media class on a dial peer.
Step 12	dial-peer voice dial-peer-tag voip Example: Device(config)# dial-peer voice 8000 voip	Configures a recorder dial peer and enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 13	destination-pattern [+] <i>string</i> [T] Example: Device(config-dial-peer)# destination-pattern 595959	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer. Keywords and arguments are as follows:
Step 14	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Configures the VoIP dial peer to use Session Initiation Protocol (SIP).
Step 15	session target ipv4: [<i>recording-server-destination-address</i> <i>recording-server-dns</i>] Example: Device(config-dial-peer)# session target ipv4:10.42.29.7	Specifies a network-specific address for a dial peer. Keyword and argument are as follows: <ul style="list-style-type: none"> • ipv4: <i>destination address</i> --IP address of the dial peer, in this format: <i>xxx.xxx.xxx.xxx</i>
Step 16	session transport tcp Example: Device(config-dial-peer)# session transport tcp	Configures a VoIP dial peer to use Transmission Control Protocol (TCP).
Step 17	end Example: Device(config-dial-peer)# end	Returns to privileged EXEC mode.

Configuration Examples for SIPREC-based Recording

Example: Configuring SIPREC-based Recording with Media Profile Recorder

```
Router> enable
Router# configure terminal
Router(config)# media class 101
Router(cfg-mediaclass)# recorder profile 201 siprec
```

Example: Configuring SIPREC-based Recording without Media Profile Recorder

```
Router> enable
Router# configure terminal
Router(config)# media class 101
Router(cfg-mediaclass)# recorder parameter siprec
Router(cfg-mediaclass-recorder)# media-recording 403
```

Validate SIPREC Functionality

Use the command **show voip rtp connections** to verify that media forking configuration is correct:

```
CUBE#show voip rtp connections
VoIP RTP active connections :
No. CallId dstCallId LocalRTP RmtRTP LocalIP RemoteIP
1 36 37 18358 19362 209.165.201.5 209.165.201.10
2 37 36 17294 17690 10.0.0.5 10.0.0.20
3 39 38 19812 42196 172.16.0.10 10.0.0.10
4 40 38 24230 60234 172.16.0.10 10.0.0.10
Found 4 active RTP connections
```

In this example, the call between the 2 phones has resulted into 2 RTP streams (1 and 2). The 2 RTP streams (3 and 4) are the recorded streams that are sent to the Recording Server (10.0.0.10 in this example). The call Recording Server receives a duplicated RTP stream that represents the recorded call. Use the command **show voip recmsp session** to verify:

```
CUBE#sh voip recmsp session
RECMSMP active sessions:
MSP Call-ID AnchorLeg Call-ID ForkedLeg Call-ID
143 141 145
Found 1 active sessions
```

To get more details of the streams run the command **show voip recmsp session detail call-id <the value specified in the above op>**:

```
CUBE#show voip recmsp session detail call-id <the value specified in the above o/p>
CUBE#show voip recmsp session detail call-id 143
RECMSMP active sessions:
Detailed Information
=====
Recording MSP Leg Details:
Call ID: 143
GUID : 7C5946D38ECD
AnchorLeg Details:
Call ID: 141
Forking Stream type: voice-nearend
Participant: 2001
Non-anchor Leg Details:
Call ID: 140
Forking Stream type: voice-farend
Participant: 1001
Forked Leg Details:
Call ID: 145
Near End Stream CallID 145
Stream State ACTIVE
Far End stream CallID 146
Stream State ACTIVE
Found 1 active sessions
```

Where:

- Stream State: This state shows the state of the call – can be either in ACTIVE or HOLD state.
- Anchor Leg Call-id: This ID is the call-id of the anchor leg (Dial-peer where forking is enabled) which is also internal to the system. The output in brief describes the participant number and stream type as voice near-end, which is called party side.
- Non-Anchor Call-id: This ID is the call-id of nonanchor leg (Dial-peer where forking is not enabled).
- Forked Call-id: This forking leg call-id shows near-end and far-end stream call-id details with state of the Stream.

If you want to know the remote IPs and ports for the near-end and far-end legs, use the **show voip rtp forking** command:

```
CUBE#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 10.0.0.10, remote port 38526, local port 18648
  codec g711ulaw, logical ssrc 0x53
  packets sent 29687, packets received 0
  stream type voice+dtmf-nearend (4): count 0
  stream type voice-farend (5): count 1
  remote ip 10.0.0.10, remote port 50482, local port 17780
  codec g711ulaw, logical ssrc 0x55
  packets sent 29686, packets received 0
  stream type voice+dtmf-farend (6): count 0
  stream type video (7): count
```

Remote IP/ Port is the recording server ip and port address. Codec indicates which codec is negotiated to record the call leg. Packets that are sent indicate the number of packets that are sent to Recording Server from each stream.

Troubleshoot

The following is a sample SIPREC configuration on IOS/IOS-XE voice routers.

```
media class 777
recorder parameter siprec
media-recording 777
!
dial-peer voice 11 voip
description CUCM
session protocol sipv2
session target ipv4:10.0.0.15
destination e164-pattern-map 164
media-class 777
codec g711ulaw
!
dial-peer voice 777 voip
destination-pattern AAAA
session protocol sipv2
session target ipv4:10.0.0.10
codec g711ulaw
```

Working Scenario

After the call is connected, the inbound/outbound CCS SIP info legs helps to understand that a recording call has been initiated. In the following example, the outbound call leg 4536 posts a media forking start indication to its peer inbound leg 4535. This inbound leg ignores this event because it is not the anchor leg (in this example, media-class command is configured on the outgoing dial peer (Peer ID 4536)).

```
017895: May 13 15:32:45.273:
//4536/2FD863BAA01F/SIP/Info/info/32768/ccsip_trigger_media_forking: MF: EO leg. set the
pending
flag. wait for peer leg to indicate start
017896: May 13 15:32:45.273:
//4536/2FD863BAA01F/SIP/Info/info/32768/ccsip_trigger_media_forking: MF: posting
CC_EV_H245_MEDIA_FORKING_START_IND.
017901: May 13 15:32:45.273: //4535/2FD863BAA01F/SIP/Info/notify/32768/ccsip_event_handler:
```

```
CC_EV_H245_MEDIA_FORKING_START_IND: peer ID 4536, event = 217 type = 1
017902: May 13 15:32:45.273: //4535/2FD863BAA01F/SIP/Info/verbose/32768/ccsip_event_handler:
Ignoring the event on non-anchor leg
```

Similarly, the outbound call leg 4536 posts a media forking start indication to the inbound call leg 5435.

```
018221: May 13 15:32:45.290: //4536/2FD863BAA01F/SIP/Info/notify/32768/ccsip_event_handler:
CC_EV_H245_MEDIA_FORKING_START_IND: peer ID 4535, event = 217 type = 1
```

Outbound leg processes the event and triggers the recording session.

```
018222: May 13 15:32:45.290: //4536/2FD863BAA01F/SIP/Info/verbose/32768/ccsip_event_handler:
Peer leg has indicated start. Trigger Media Forking.
```

```
018229: May 13 15:32:45.290: //-1/xxxxxxxxxxxx/Event/recmsp_api_create_session: Event:
E_REC_CREATE_SESSION anchor call ID:4536, msp call ID:4537
018230: May 13 15:32:45.290: //-1/xxxxxxxxxxxx/Inout/recmsp_api_create_session: Exit with
Success
```

Recording dial-peer lookup.

```
018320: May 13 15:32:45.293: //4537/2FD863BAA01F/REC MSP/Inout/recmsp_get_dp_tag_list: REC
DP: =
777
018390: May 13 15:32:45.296: //-
1/xxxxxxxxxxxx/SIP/Info/verbose/5120/sipSPIGetOutboundHostAndDestHostPrivate: CCSIP:
target_host
: 10.0.0.10 target_port : 5060
```

Create XML metadata.

```
018513: May 13 15:32:45.301:
//4538/2FD863BAA01F/SIP/Info/info/32768/ccsip_ipip_mf_create_xml_metadata: MF: XML metadata
Len:
[1763]
<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
<datamode>complete</datamode>
<session session_id="MIgZ2nTLEemWFaQilvyb4Q==">
<sipSessionID>a0b9b2a1e4db51f082e777c0df9015e5;remote=6bea155500105000a0002c31246a214b</sipSessi
onID>
<start-time>2019-05-13T15:32:45.293Z</start-time>
</session>
<participant participant_id="MIhBMXTLEemWFqQilvyb4Q==">
<nameID aor="sip:1234@10.0.0.15">
</nameID>
</participant>
<participantses**MSG 00003 TRUNCATED**
**MSG 00003 CONTINUATION #01**sionassoc participant_id="MIhBMXTLEemWFqQilvyb4Q=="
session_id="MIgZ2nTLEemWFaQilvyb4Q==">
<associate-time>2019-05-13T15:32:45.293Z</associate-time>
</participantsessionassoc>
<stream stream_id="MIlSKnTLEemWG6Qilvyb4Q==" session_id="MIgZ2nTLEemWFaQilvyb4Q==">
<label>1</label>
</stream>
<participant participant_id="MIhBMXTLEemWF6Qilvyb4Q==">
<nameID aor="sip:911@209.165.201.1">
<name xml:lang="en">Emergency</name>
</nameID>
</participant>
<participantsessionassoc participant_id="MIhBMXTLEemWF6Qilvyb4Q=="
session_id="MIgZ2nTLEemWFaQilvyb4Q==">
<asso**MSG 00003 TRUNCATED**
**MSG 00003 CONTINUATION #02**ciate-time>2019-05-13T15:32:45.293Z</associate-time>
</participantsessionassoc>
<stream stream_id="MIlSKnTLEemWHKQilvyb4Q==" session_id="MIgZ2nTLEemWFaQilvyb4Q==">
<label>2</label>
```



```

</stream>
<participantstreamassoc participant_id="MIhBMXTLEemWFqQilvyb4Q==">
<send>MIlSKnTLEemWG6Qilvyb4Q==</send>
<recv>MIlSKnTLEemWHKQilvyb4Q==</recv>
</participantstreamassoc>
<participantstreamassoc participant_id="MIhBMXTLEemWF6Qilvyb4Q==">
<send>MIlSKnTLEemWHKQilvyb4Q==</send>
<recv>MIlSKnTLEemWG6Qilvyb4Q==</recv>
</participantstreamassoc>
</recording>

```

INVITE is sent to recorder with metadata in XML format where:

- The **nameID** attribute represents the name and SIP/SIPS/tel URI (also called the address of record) of each participant.
- The **participant_id** attribute indicates the unique ID assigned to each participant in the recording session.
- The **stream_id** attribute indicates the unique ID assigned to each media stream in the recording session.
- The **session_id** attribute is used to reference the communication session to which a given media stream belongs.
- The label metadata attribute provides the value of **a=label** attribute assigned to this media stream in the SDP of the SIP request and responses of the recording session. It plays a key role in associating a media stream with its metadata information.

```
018628: May 13 15:32:45.306: //4538/2FD863BAA01F/SIP/Msg/ccsipDisplayMsg:
```

```
Sent:
```

```
INVITE sip:AAAA@10.0.0.10:5060 SIP/2.0
```

```
Via: SIP/2.0/UDP y.y.y.y:5060;branch=z9hG4bK11BD2CA
```

```
From: <sip:y.y.y.y>;tag=F75AD7F-2065
```

```
To: <sip:AAAA@10.0.0.10>
```

```
Date: Mon, 13 May 2019 15:32:45 GMT
```

```
Call-ID: 3089C795-74CB11E9-961DA422-D6FC9BE1@y.y.y.y
```

```
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
```

```
Require: siprec
```

```
Min-SE: 1800
```

```
Cisco-Guid: 0802710458-1959465449-2686421522-1015028268
```

```
User-Agent: Cisco-SIPGateway/IOS-16.10.2
```

```
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
```

```
CSeq: 101 INVITE
```

```
Max-Forwards: 70
```

```
Timestamp: 1557761565
```

```
Contact: <sip:y.y.y.y:5060>;+sip.src
```

```
Expires: 180
```

```
Allow-Events: telephone-event
```

```
Session-ID: a62dd6d8be0059c38d142bae9b46880b;remote=00000000000000000000000000000000
```

```
Session-Expires: 1800
```

```
Content-Type: multipart/mixed;boundary=uniqueBoundary
```

```
Mime-Version: 1.0
```

```
Content-Length: 2470
```

```
--uniqueBoundary
```

```
Content-Type: application/sdp
```

```
Content-Disposition: session;handling=required
```

```
v=0
```

```
o=CiscoSystemsSIP-GW-UserAgent 5511 2889 IN IP4 y.y.y.y
```

```
s=SIP Call
```

```
c=IN IP4 y.y.y.y
```

```
t=0 0
```

```
m=audio 8086 RTP/AVP 0 101 19
```

```
c=IN IP4 y.y.y.y
```

```

a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
aptime:20
a=sendonly
a=label:1
m=audio 8088 RTP/AVP 0 101 19
c=IN IP4 y.y.y.y
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
aptime:20
a=sendonly
a=label:2
--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session
<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
  <datamode>complete</datamode>
  <session session_id="MIgZ2nTLEemWfAQilvyb4Q==">
<sipSessionID>a0b9b2a1e4db51f082e777c0df9015e5;remote=6bea155500105000a0002c31246a214b</sipSessi
onID>
<start-time>2019-05-13T15:32:45.293Z</start-time> </session>
<participant participant_id="MIhBMXTLEemWFqQilvyb4Q==">
<nameID aor="sip:1234@10.0.0.15">
</nameID>
</participant>
<participantsessionassoc participant_id="MIhBMXTLEemWFqQilvyb4Q=="
  session_id="MIgZ2nTLEemWfAQilvyb4Q==">
  <associate-time>2019-05-13T15:32:45.293Z</associate-time>
</participantsessionassoc>
<stream stream_id="MIlSKnTLEemWG6Qilvyb4Q==" session_id="MIgZ2nTLEemWfAQilvyb4Q==">
<label>1</label>
</stream>
<participant participant_id="MIhBMXTLEemWF6Qilvyb4Q==">
  <nameID aor="sip:911@209.165.201.1">
  <name xml:lang="en">Emergency</name>
  </nameID>
</participant>
<participantsessionassoc participant_id="MIhBMXTLEemWF6Qilvyb4Q=="
  session_id="MIgZ2nTLEemWfAQilvyb4Q==">
  <associate-time>2019-05-13T15:32:45.293Z</associate-time>
</participantsessionassoc>
<stream stream_id="MIlSKnTLEemWHKQilvyb4Q==" session_id="MIgZ2nTLEemWfAQilvyb4Q==">
  <label>2</label>
</stream>
<participantstreamassoc participant_id="MIhBMXTLEemWFqQilvyb4Q==">
  <send>MIlSKnTLEemWG6Qilvyb4Q==</send>
  <recv>MIlSKnTLEemWHKQilvyb4Q==</recv>
</participantstreamassoc>
<participantstreamassoc participant_id="MIhBMXTLEemWF6Qilvyb4Q==">
  <send>MIlSKnTLEemWHKQilvyb4Q==</send>
  <recv>MIlSKnTLEemWG6Qilvyb4Q==</recv>
</participantstreamassoc>
</recording>
--uniqueBoundary--

```

In 200 OK recorder sends media **a=recvonly** and media forking is started.

```

018638: May 13 15:32:45.307: //4538/2FD863BAA01F/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP y.y.y.y:5060;branch=z9hG4bK11BD2CA
From: <sip:y.y.y.y>;tag=F75AD7F-2065
To: <sip:AAAA@10.0.0.10>;tag=7
Call-ID: 3089C795-74CB11E9-961DA422-D6FC9BE1@y.y.y.y
CSeq: 101 INVITE
Contact: <sip:10.0.0.10:5060;transport=UDP>
Content-Type: application/sdp
Content-Length: 207
v=0
o=user1 53655765 2353687637 IN IP4 10.0.0.10
s=-
c=IN IP4 10.0.0.10
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=recvonly
m=audio 8002 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=recvonly
018809: May 13 15:32:45.313: //4537/2FD863BAA01F/RECMSP/Event/recmsp_api_connect: Event:
E_REC_CC_CONNECTmsp call ID:4537 in recmsp_api_connect

```

Nonworking Scenarios

The issue of recording not being initiated by CUBE is reported in new deployments, and the primary root cause is incorrect configuration. The following are some examples:

- There is an incorrect inbound dial-peer match (that is, the selected inbound dial peer does not have media-class associated with it).
- The destination-pattern in the recording dial peer is a regular expression pattern instead of a simple directory number (1... instead of 1234)
- There is an incorrect Recording Server IP address or the server's hostname is not successfully resolved to an IP address.

One of the reasons for failures in postproduction deployments are due to Recording Server not available or unreachable. SIP responses such as **503 Service Unavailable** and **500 Server Internal Error** are received in response to the INVITE from the Recording Server. In such situations, add **debug ip tcp transactions** to the debug command list to determine whether TCP connections are getting established correctly.

In other circumstances, recording files could be missing. Verify that CUBE transmits RTP packets to the Recording Server while a call is recorded. Alternatively, you can obtain Packet Captures using Embedded Packet Capture on the Router side and Wireshark at the server side.

There are useful debugs to troubleshoot SIPREC on CUBE.

```

debug voip ccapi inout
debug ccsip message
debug ccsip events
debug ccsip error
debug ccsip info
debug voip recmsp event
debug voip recmsp error debug voip recmsp inout

```

Configuration Example for Metadata Variations with Different Mid-call Flows

Example: Complete SIP Recording Metadata Information Sent in INVITE or Re-INVITE

The following example provides all the elements involved in Recording Metadata XML body.

```
--uniqueBoundary
Content-Type: application/sdp
Content-Disposition: session;handling=required
v=0
o=CiscoSystemsSIP-GW-UserAgent 509 7422 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16552 RTP/AVP 8 101
c=IN IP4 9.42.25.149
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
aptime:20
a=sendonly
a=label:1
m=audio 16554 RTP/AVP 8 101
c=IN IP4 9.42.25.149
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
aptime:20
a=sendonly
a=label:2
m=video 16556 RTP/AVP 119
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:119 H264/90000
a=fmtp:119 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:3
m=video 16558 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:4
--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
  <datamode>complete</datamode>
  <session session_id="JaPQePlCEeSA66sYHx7YVg==">
    <sipSessionID>276ac102a3c05270a4375d99512ea1a1;remote=110b0c0f50775078b13d60be0044db11
    </sipSessionID>
    <start-time>2015-05-19T09:42:06.911Z</start-time>
  </session>
</recording>
```

```

</session>
<participant participant_id="JaPQeP1CEeSA76sYHx7YVg==">
  <nameID aor="sip:808808@9.0.0.174">
    <name xml:lang="en">808808</name>
  </nameID>
</participant>
<participantsessionassoc participant_id="JaPQeP1CEeSA76sYHx7YVg=="
session_id="JaPQeP1CEeSA66sYHx7YVg==">
  <associate-time>2015-05-19T09:42:06.911Z</associate-time>
</participantsessionassoc>
<stream stream_id="JaPQeP1CEeSA8KsYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg==">
  <label>1</label>
</stream>
<stream stream_id="JaPQeP1CEeSA8asYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg==">
  <label>3</label>
</stream>
<participant participant_id="JaPQeP1CEeSA8qsYHx7YVg==">
  <nameID aor="sip:909909@9.0.0.174">
    <name xml:lang="en">909909</name>
  </nameID>
</participant>
<participantsessionassoc participant_id="JaPQeP1CEeSA8qsYHx7YVg=="
session_id="JaPQeP1CEeSA66sYHx7YVg==">
  <associate-time>2015-05-19T09:42:06.911Z</associate-time>
</participantsessionassoc>
<stream stream_id="JaPQeP1CEeSA86sYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg==">
  <label>2</label>
</stream>
<stream stream_id="JaPQeP1CEeSA9KsYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg==">
  <label>4</label>
</stream>
<participantstreamassoc participant_id="JaPQeP1CEeSA76sYHx7YVg==">
  <send>JaPQeP1CEeSA8KsYHx7YVg==</send>
  <recv>JaPQeP1CEeSA86sYHx7YVg==</recv>
  <send>JaPQeP1CEeSA8asYHx7YVg==</send>
  <recv>JaPQeP1CEeSA9KsYHx7YVg==</recv>
</participantstreamassoc>
<participantstreamassoc participant_id="JaPQeP1CEeSA8qsYHx7YVg==">
  <send>JaPQeP1CEeSA86sYHx7YVg==</send>
  <recv>JaPQeP1CEeSA8KsYHx7YVg==</recv>
  <send>JaPQeP1CEeSA9KsYHx7YVg==</send>
  <recv>JaPQeP1CEeSA8asYHx7YVg==</recv>
</participantstreamassoc>
</recording>
-uniqueBoundary-

```

Output Field	Description
urn:ietf:params:xml:ns:recording:1	Defines the namespace URI for the elements—Uniform Resource Namespace (URN).
datamode>complete</datamode	<dataMode> is a recording element that indicates whether the XML document is a complete document or a partial update. If no <dataMode> element is present then the default value is "complete".
session session_id="JaPQeP1CEeSA66sYHx7YVg=="	Session ID which remains constant for the complete call leg.

Output Field	Description
<pre>sipSessionID 276ac102a3c05270a4375d99512ea1a1; remote=110b0c0f50775078b13d60be0044db11</pre>	<p>This attribute carries a SIP Session-ID of the original call between the participants.</p>
<pre><participant participant_id="JaPQeP1CEeSA76sYHx7YVg=="> <nameID aor="sip:808808@9.0.0.174"></pre>	<p>Name and participant ID of the first participant. The first participant will always be the anchor leg of the call. Each participant has a unique 'participant_id' attribute. For example, nameID is sip:808808.</p>
<pre>a=label:1; <stream stream_id="JaPQeP1CEeSA86sYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg=="> <label>1</label> </stream></pre>	<p>The <stream> element represents a Media Stream object. Stream element indicates the SDP media lines associated with the session and participants.</p> <p>The <label> element within the <stream> element references an SDP "a=label" attribute that identifies an m-line within the RS SDP. This m-line carries the media stream from the SRC to the SRS.</p>
<pre>participantsessionassoc participant_id="JaPQeP1CEeSA76sYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg=="></pre>	<p>Participant CS Association class describes the association of the first participant to a CS for a period of time. A participant can associate and dissociate from a CS several times.</p> <p>ParticipantCS association class has the following attributes:</p> <ul style="list-style-type: none"> • Associate-time—Time when the participant is associated to CS. • Disassociate-time—Time when the participant is disassociated from a CS. <p>Each CS object is represented by one session element. Each session element has a unique 'session_id' attribute which helps to identify unique CS sessions.</p>
<pre>participantsessionassoc participant_id="JaPQeP1CEeSA8qsYHx7YVg==" session_id="JaPQeP1CEeSA66sYHx7YVg=="></pre>	<p>Participant CS Association class describes the association of the second participant to a CS for a period of time. A participant can associate and dissociate from a CS several times.</p> <p>The 'session_id' attribute helps to identify unique CS session of the second participant.</p>

Output Field	Description
<pre>participantstreamassoc participant_id="JaPQeP1CEeSA76sYHx7YVg=="; participantstreamassoc participant_id="JaPQeP1CEeSA8qsYHx7YVg==";</pre>	<p>Participant stream association class describes the association of either participant 1 or 2 to a media stream for a period of time, as a sender or as a receiver, or both. These streams can be either audio or video or both.</p> <p>ParticipantStream association class has the following attributes:</p> <ul style="list-style-type: none"> • Associate-time—Time when the participant starts contributing for a media stream. • Disassociate-time—Time when the participant stops receiving a media stream.

Example: Hold with Send-only / Recv-only Attribute in SDP

When a participant puts the audio call on hold with send-only attribute, the stream is sent only in one direction.

Here, in a normal recording session, both participants sent audio and video streams.

```
--uniqueBoundary
Content-Type: application/sdp
Content-Disposition: session;handling=required

v=0
o=CiscoSystemsSIP-GW-UserAgent 2973 4879 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16464 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:1
m=audio 16466 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:2
m=video 16468 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:3
m=video 16470 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
```

Example: Hold with Send-only / Recv-only Attribute in SDP

```

a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="jIBTUf1BEeSAdKsYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>1</label>
  </stream>
  <stream stream_id="jIBTUf1BEeSAdasYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>3</label>
  </stream>
...
  <stream stream_id="jIBTUf1BEeSAd6sYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>2</label>
  </stream>
  <stream stream_id="jIBTUf1BEeSAeKsYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>4</label>
  </stream>
  <participantstreamassoc participant_id="jIBTUf1BEeSAc6sYHx7YVg==">
    <send>jIBTUf1BEeSAdKsYHx7YVg==</send>
    <recv>jIBTUf1BEeSAd6sYHx7YVg==</recv>
    <send>jIBTUf1BEeSAdasYHx7YVg==</send>
    <recv>jIBTUf1BEeSAeKsYHx7YVg==</recv>
  </participantstreamassoc>
  <participantstreamassoc participant_id="jIBTUf1BEeSAdqsYHx7YVg==">
    <send>jIBTUf1BEeSAd6sYHx7YVg==</send>
    <recv>jIBTUf1BEeSAdKsYHx7YVg==</recv>
    <send>jIBTUf1BEeSAeKsYHx7YVg==</send>
    <recv>jIBTUf1BEeSAdasYHx7YVg==</recv>
  </participantstreamassoc>
</recording>

--uniqueBoundary--

```

In this scenario, the second participant puts the call on hold using `sendonly` and the first participant will respond using `recvonly`. You can see from the **participantStream association** element that the second participant only sends audio and video streams and the first participant just receives the media streams.

The output after the second participant puts the call on hold with `sendonly` attribute:

```

--uniqueBoundary
Content-Type: application/sdp

v=0
o=CiscoSystemsSIP-GW-UserAgent 2973 4880 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16464 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=inactive
a=label:1
m=audio 16466 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000

```



```

a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:2
m=video 16468 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=inactive
a=label:3
m=video 16470 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="jIBTUf1BEeSAdKsYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>1</label>
  </stream>
  <stream stream_id="jIBTUf1BEeSAdasYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>3</label>
  </stream>
...
  <stream stream_id="jIBTUf1BEeSAd6sYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>2</label>
  </stream>
  <stream stream_id="jIBTUf1BEeSAeKsYHx7YVg==" session_id="jH+2kf1BEeSAb6sYHx7YVg==">
    <label>4</label>
  </stream>
  <participantstreamassoc participant_id="jIBTUf1BEeSAc6sYHx7YVg==">
    <recv>jIBTUf1BEeSAd6sYHx7YVg==</recv>
    <recv>jIBTUf1BEeSAeKsYHx7YVg==</recv>
  </participantstreamassoc>
  <participantstreamassoc participant_id="jIBTUf1BEeSAdqsYHx7YVg==">
    <send>jIBTUf1BEeSAd6sYHx7YVg==</send>
    <send>jIBTUf1BEeSAeKsYHx7YVg==</send>
  </participantstreamassoc>
</recording>

--uniqueBoundary--

```

Example: Hold with Inactive Attribute in SDP

Here, you can see that video call is sent in the initial INVITE to recorder where both the participants send and receive audio and video streams. There are 2 audio and 2 video streams from both the participants each in the **participantStream association** element.

```

--uniqueBoundary
Content-Type: application/sdp
Content-Disposition: session;handling=required

v=0

```

```

o=CiscoSystemsSIP-GW-UserAgent 7476 1347 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16496 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:1
m=audio 16498 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:2
m=video 16500 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:3
m=video 16502 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="uV/B4f1BEeSAmKsYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
    <label>1</label>
  </stream>
  <stream stream_id="uV/B4f1BEeSAmasYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
    <label>3</label>
  </stream>
...
  <stream stream_id="uV/B4f1BEeSAm6sYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
    <label>2</label>
  </stream>
  <stream stream_id="uV/B4f1BEeSAnKsYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
    <label>4</label>
  </stream>
  <participantstreamassoc participant_id="uV/B4f1BEeSA16sYHx7YVg==">
    <send>uV/B4f1BEeSAmKsYHx7YVg==</send>
    <recv>uV/B4f1BEeSAm6sYHx7YVg==</recv>
    <send>uV/B4f1BEeSAmasYHx7YVg==</send>
    <recv>uV/B4f1BEeSAnKsYHx7YVg==</recv>
  </participantstreamassoc>
  <participantstreamassoc participant_id="uV/B4f1BEeSAmqsYHx7YVg==">
    <send>uV/B4f1BEeSAm6sYHx7YVg==</send>
    <recv>uV/B4f1BEeSAmKsYHx7YVg==</recv>
  </participantstreamassoc>

```

```

        <send>uV/B4f1BEeSAnKsYHx7YVg==</send>
        <recv>uV/B4f1BEeSAmasYHx7YVg==</recv>
    </participantstreamassoc>
</recording>

--uniqueBoundary--

```

When the first participant puts the call on hold with inactive SDP attribute, there will be not any active streams in the metadata.

```

--uniqueBoundary
Content-Type: application/sdp

v=0
o=CiscoSystemsSIP-GW-UserAgent 7476 1348 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16496 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=inactive
a=label:1
m=audio 16498 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=inactive
a=label:2
m=video 16500 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=inactive
a=label:3
m=video 16502 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=inactive
a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
    <stream stream_id="uV/B4f1BEeSAnKsYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
        <label>1</label>
    </stream>
    <stream stream_id="uV/B4f1BEeSAmasYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
        <label>3</label>
    </stream>
...
    <stream stream_id="uV/B4f1BEeSAm6sYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
        <label>2</label>

```

```

</stream>
<stream stream_id="uV/B4f1BEeSAnKsYHx7YVg==" session_id="uV/B4f1BEeSAk6sYHx7YVg==">
  <label>4</label>
</stream>
<participantstreamassoc participant_id="uV/B4f1BEeSAl6sYHx7YVg==">
</participantstreamassoc>
<participantstreamassoc participant_id="uV/B4f1BEeSAmqsYHx7YVg==">
</participantstreamassoc>
</recording>

--uniqueBoundary--

```

Example: Escalation

During escalation, video streams will be added to the Re-INVITE meta-data sent to the recorder.

In the below example, you can see the metadata representation of an original audio call sent in the initial INVITE to the recorder where both the participants send and receive audio streams.

```

--uniqueBoundary
Content-Type: application/sdp
Content-Disposition: session;handling=required

v=0
o=CiscoSystemsSIP-GW-UserAgent 6360 4788 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16628 RTP/AVP 8 101
c=IN IP4 9.42.25.149
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:1
m=audio 16630 RTP/AVP 8 101
c=IN IP4 9.42.25.149
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:2

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="evyS5/1CEeSBOKsYHx7YVg==" session_id="evv2v/1CEeSBM6sYHx7YVg==">
    <label>1</label>
  </stream>
...
  <stream stream_id="evyS5/1CEeSBOqsYHx7YVg==" session_id="evv2v/1CEeSBM6sYHx7YVg==">
    <label>2</label>
  </stream>
  <participantstreamassoc participant_id="evyS5/1CEeSBN6sYHx7YVg==">
    <send>evyS5/1CEeSBOKsYHx7YVg==</send>
    <recv>evyS5/1CEeSBOqsYHx7YVg==</recv>
  </participantstreamassoc>

```

```

    <participantstreamassoc participant_id="evyS5/1CEeSBOasYHx7YVg==">
      <send>evyS5/1CEeSBOqsYHx7YVg==</send>
      <recv>evyS5/1CEeSBOKsYHx7YVg==</recv>
    </participantstreamassoc>
  </recording>

```

```
--uniqueBoundary--
```

After escalation, video streams get added into the **participantStream association** element in metadata for both the participants. There will be 4 streams in total.

```

--uniqueBoundary
Content-Type: application/sdp

v=0
o=CiscoSystemsSIP-GW-UserAgent 6360 4789 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16628 RTP/AVP 18 101
c=IN IP4 9.42.25.149
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:1
m=audio 16630 RTP/AVP 18 101
c=IN IP4 9.42.25.149
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:2
m=video 16636 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:3
m=video 16638 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="evyS5/1CEeSBOKsYHx7YVg==" session_id="evv2v/1CEeSBM6sYHx7YVg==">
    <label>1</label>
  </stream>
  <stream stream_id="e5Zhtv1CEeSBPKsYHx7YVg==" session_id="evv2v/1CEeSBM6sYHx7YVg==">
    <label>3</label>
  </stream>

```

```

...
<stream stream_id="e5Zhtv1CEeSBPasYHx7YVg==" session_id="evv2v/1CEeSBM6sYHx7YVg==">
  <label>4</label>
</stream>
<participantstreamassoc participant_id="evyS5/1CEeSBN6sYHx7YVg==">
  <send>evyS5/1CEeSBOKsYHx7YVg==</send>
  <recv>evyS5/1CEeSBOqsYHx7YVg==</recv>
  <send>e5Zhtv1CEeSBPKsYHx7YVg==</send>
  <recv>e5Zhtv1CEeSBPasYHx7YVg==</recv>
</participantstreamassoc>
<participantstreamassoc participant_id="evyS5/1CEeSBOasYHx7YVg==">
  <send>evyS5/1CEeSBOqsYHx7YVg==</send>
  <recv>evyS5/1CEeSBOKsYHx7YVg==</recv>
  <send>e5Zhtv1CEeSBPasYHx7YVg==</send>
  <recv>e5Zhtv1CEeSBPKsYHx7YVg==</recv>
</participantstreamassoc>
</recording>

--uniqueBoundary--

```

Example: De-escalation

During de-escalation, video streams will be truncated in the Re-INVITE metadata sent to the recorder.

In the below example, you can see two streams each for the audio and video calls in the metadata.

```

--uniqueBoundary
Content-Type: application/sdp
Content-Disposition: session;handling=required

v=0
o=CiscoSystemsSIP-GW-UserAgent 7616 8308 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16648 RTP/AVP 116 101
c=IN IP4 9.42.25.149
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=maxptime:20
a=sendonly
a=label:1
m=audio 16650 RTP/AVP 116 101
c=IN IP4 9.42.25.149
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=maxptime:20
a=sendonly
a=label:2
m=video 16652 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:3
m=video 16654 RTP/AVP 97

```

```

c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="j50QdP1CEeSBSqsYHx7YVg==" session_id="j5L0TP1CEeSBRasYHx7YVg==">
    <label>1</label>
  </stream>
  <stream stream_id="j50QdP1CEeSBS6sYHx7YVg==" session_id="j5L0TP1CEeSBRasYHx7YVg==">
    <label>3</label>
  </stream>
...
  <stream stream_id="j50QdP1CEeSBTasYHx7YVg==" session_id="j5L0TP1CEeSBRasYHx7YVg==">
    <label>2</label>
  </stream>
  <stream stream_id="j50QdP1CEeSBTqsYHx7YVg==" session_id="j5L0TP1CEeSBRasYHx7YVg==">
    <label>4</label>
  </stream>
  <participantstreamassoc participant_id="j50QdP1CEeSBSasYHx7YVg==">
    <send>j50QdP1CEeSBSqsYHx7YVg==</send>
    <recv>j50QdP1CEeSBTasYHx7YVg==</recv>
    <send>j50QdP1CEeSBS6sYHx7YVg==</send>
    <recv>j50QdP1CEeSBTqsYHx7YVg==</recv>
  </participantstreamassoc>
  <participantstreamassoc participant_id="j50QdP1CEeSBTKsYHx7YVg==">
    <send>j50QdP1CEeSBTasYHx7YVg==</send>
    <recv>j50QdP1CEeSBSqsYHx7YVg==</recv>
    <send>j50QdP1CEeSBTqsYHx7YVg==</send>
    <recv>j50QdP1CEeSBS6sYHx7YVg==</recv>
  </participantstreamassoc>
</recording>

--uniqueBoundary--

```

After de-escalation, video streams are removed from the metadata and only audio calls will be present in the **participantStream association** element.

```

--uniqueBoundary
Content-Type: application/sdp

v=0
o=CiscoSystemsSIP-GW-UserAgent 7616 8309 IN IP4 9.42.25.149
s=SIP Call
c=IN IP4 9.42.25.149
t=0 0
m=audio 16648 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:1
m=audio 16650 RTP/AVP 0 101
c=IN IP4 9.42.25.149
a=rtpmap:0 PCMU/8000

```

```

a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=sendonly
a=label:2
m=video 0 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:3
m=video 0 RTP/AVP 97
c=IN IP4 9.42.25.149
b=TIAS:1000000
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801E;packetization-mode=0
a=sendonly
a=label:4

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
...
  <stream stream_id="j50QdP1CEeSBSqsYHx7YVg==" session_id="j5L0TP1CEeSBRasYHx7YVg==">
    <label>1</label>
  </stream>
...
  <stream stream_id="j50QdP1CEeSBTasYHx7YVg==" session_id="j5L0TP1CEeSBRasYHx7YVg==">
    <label>2</label>
  </stream>
  <participantstreamassoc participant_id="j50QdP1CEeSBSasYHx7YVg==">
    <send>j50QdP1CEeSBSqsYHx7YVg==</send>
    <recv>j50QdP1CEeSBTasYHx7YVg==</recv>
  </participantstreamassoc>
  <participantstreamassoc participant_id="j50QdP1CEeSBTKsYHx7YVg==">
    <send>j50QdP1CEeSBTasYHx7YVg==</send>
    <recv>j50QdP1CEeSBSqsYHx7YVg==</recv>
  </participantstreamassoc>
</recording>

--uniqueBoundary--

```

Configuration Example for Metadata Variations with Different Transfer Flows

Example: Transfer of Re-INVITE/REFER Consume Scenario

In the case of Re-INVITE or REFER Consume transfer scenarios, CUBE receives re-INVITE with caller-id change. This re-INVITE will have the remote-party-ID details.

After transfer, participant A is disassociated from the call and participant C joins the call. This information is provided in the metadata sent to the recording server. Here, **7774442214** associates and **7774442212** disassociates from the call.


```

INVITE sip:7774442216@10.64.86.102:5060;transport=tcp SIP/2.0
From: <sip:7774442212@10.104.54.52>;tag=498652~97a89a01
To: <sip:7774442216@10.64.86.102>;tag=7C798-1441
...
...
Remote-Party-ID: <sip:7774442214@10.104.54.52>;party=calling;screen=yes;privacy=off
Contact: <sip:7774442214@10.104.54.52:5060;transport=tcp>
...
<participant participant_id="vm+z2xM6EeWAIN4iOrLrag==">
  <nameID aor="sip:7774442214@10.104.54.52">
    </nameID>
  </participant>
  <participantsessionassoc participant_id="vm+z2xM6EeWAIN4iOrLrag=="
session_id="vACJ+xM6EeWAF94iOrLrag==">
  <associate-time>2015-06-16T08:44:32.869Z</associate-time>
  </participantsessionassoc>
...
<participant participant_id="vACJ+xM6EeWAGN4iOrLrag==">
  <nameID aor="sip:7774442212@10.104.54.52">
    </nameID>
  </participant>
  <participantsessionassoc participant_id="vACJ+xM6EeWAGN4iOrLrag=="
session_id="vACJ+xM6EeWAGN4iOrLrag==">
  <disassociate-time>2015-06-16T08:44:32.869Z</disassociate-time>
  </participantsessionassoc>
...

```

Configuration Examples for Metadata Variations with Caller-ID UPDATE Flow

Example: Caller-ID UPDATE Request and Response Scenario

In case of Re-INVITE based transfer, any UPDATE request will contain caller-id changes. These changes are forwarded to the remote party and once CUBE receives a 200OK message, the remote-party-ID details are transferred.

The response of UPDATE request contains the associated caller-id changes. The CUBE forwards the response UPDATE information to the remote party with caller-id changes after the UPDATE request. From the metadata, you can see that the participants A and C disassociate from the call and participants B and D joins (associates) the call. Here, **7774442212** and **7774442216** disassociates from the call and **7774442214** and **7774442218** joins the call after the caller-id update.

```

UPDATE sip:7774442216@10.64.86.102:5060;transport=tcp SIP/2.0
From: <sip:7774442212@10.104.54.52>;tag=498652~97a89a01
To: <sip:7774442216@10.64.86.102>;tag=7C798-1441
...
...
Remote-Party-ID: <sip:7774442214@10.104.54.52>;party=calling;screen=yes;privacy=off
Contact: <sip:7774442214@10.104.54.52:5060;transport=tcp>

Response of UPDATE contains caller-id changes
...
SIP/2.0 200 OK
From: <sip:7774442212@10.64.86.102>;tag=7C78C-1E7C
To: <sip:7774442216@10.104.54.52>;tag=498653~97a89a01
...
Remote-Party-ID: <sip:7774442218@10.104.54.52>;party=called;screen=yes;privacy=off

```

```

Contact: <sip:7774442218@10.104.54.52:5060>
Content-Length: 0

...
  <participant participant_id="vm+z2xM6EeWAIN4iOrLrag==">
    <nameID aor="sip:7774442214@10.104.54.52">
      </nameID>
    </participant>
    <participantsessionassoc participant_id="vm+z2xM6EeWAIN4iOrLrag=="
session_id="vACJ+xM6EeWAF94iOrLrag==">
      <associate-time>2015-06-16T08:44:32.869Z</associate-time>
    </participantsessionassoc>
    <participant participant_id="vm+z2xM6EeWAIN4iOrLrag==">
      <nameID aor="sip:7774442218@10.104.54.52">
        </nameID>
      </participant>
    <participantsessionassoc participant_id="vm+z2xM6EeWAIN4iOrLrag=="
session_id="vACJ+xM6EeWAF94iOrLrag==">
      <associate-time>2015-06-16T08:44:32.869Z</associate-time>
    </participantsessionassoc>
    <participant participant_id="vACJ+xM6EeWAGN4iOrLrag==">
      <nameID aor="sip:7774442212@10.104.54.52">
        </nameID>
      </participant>
    <participantsessionassoc participant_id="vACJ+xM6EeWAGN4iOrLrag=="
session_id="vACJ+xM6EeWAGN4iOrLrag==">
      <disassociate-time>2015-06-16T08:44:32.869Z</disassociate-time>
    </participantsessionassoc>
    <participant participant_id="vACJ+xM6EeWAGN4iOrLrag==">
      <nameID aor="sip:7774442216@10.104.54.52">
        </nameID>
      </participant>
    <participantsessionassoc participant_id="vACJ+xM6EeWAGN4iOrLrag=="
session_id="vACJ+xM6EeWAGN4iOrLrag==">
      <disassociate-time>2015-06-16T08:44:32.869Z</disassociate-time>
    </participantsessionassoc>
...

```

Configuration Example for Metadata Variations with Call Disconnect

Example: Disconnect while Sending Metadata with BYE

When the original call disconnects without any reason, CUBE initiates a BYE session with the recording server along with the metadata.

In this case, the metadata contains the end time of the session along with the disassociation time of all the active participants from the call.

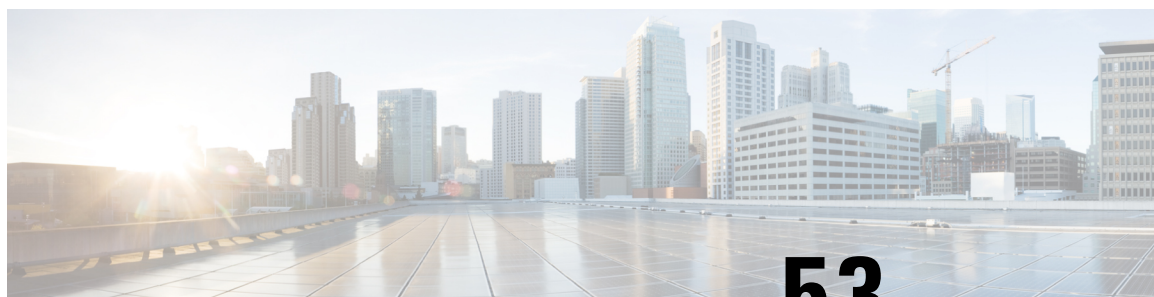
```

BYE sip:5555555@8.41.17.71:13961;transport=UDP SIP/2.0
...
Reason: Q.850;cause=16
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session
Content-Length: 984

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">

```

```
<datamode>complete</datamode>
<session session_id="t5nW8RM6EeWACN4iOrLrag==">
  <end-time>2015-06-16T08:44:36.661Z</end-time>
</session>
<participant participant_id="t5nW8RM6EeWACt4iOrLrag==">
  <nameID aor="sip:7774442212@10.104.54.52">
    </nameID>
  </participant>
  <participantsessionassoc participant_id="t5nW8RM6EeWACt4iOrLrag=="
session_id="t5nW8RM6EeWACt4iOrLrag==">
    <disassociate-time>2015-06-16T08:44:36.657Z</disassociate-time>
  </participantsessionassoc>
  <participant participant_id="t5nW8RM6EeWACd4iOrLrag==">
    <nameID aor="sip:7774442214@10.104.54.52">
      </nameID>
    </participant>
    <participantsessionassoc participant_id="t5nW8RM6EeWACd4iOrLrag=="
session_id="t5nW8RM6EeWACd4iOrLrag==">
      <disassociate-time>2015-06-16T08:44:36.657Z</disassociate-time>
    </participantsessionassoc>
  </recording>
```

CHAPTER 53

Video Recording

- [Overview, on page 531](#)
- [Configure Video Forking, on page 532](#)
- [Verify for Video Forking, on page 535](#)

Overview

This module describes the following additional configurations that can be done for Video Recording:

- Request a Full-Intra Frame using RTCP or SIP INFO methods.
- Configure an H.264 Packetization mode.
- Monitor Intra-Frames and Reference Frames

Feature Information

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 74: Feature Information for Network-Based Recording of Video Calls Using Cisco Unified Border Element

Feature Name	Releases	Feature Information
Network-Based Recording of Video Calls Using Cisco Unified Border Element	Baseline Functionality	The following commands were introduced or modified: media profile video , ref-frame-req rtcp , ref-frame-req sip-info , video profile , h264-packetization-mode , monitor-ref-frames .

Full Intra-Frame Request

Full Intra-Frame Request is a request sent for an I-frame. An I-frame is an entire key or reference frame that is compressed without considering preceding or succeeding video frames. Succeeding video frames are differences to the original I-frame (what has moved) instead of entire video frame information.

The call between Cisco Unified Border Element and the Cisco MediaSense server is established after the call between the endpoints is established. As a result, the Real-Time Transport Protocol (RTP) channel between the endpoints gets established first and the RTP channel with the recording server gets established later. The impact of this delay is more on video recording because the initial I-frame from the endpoint may not get forked, and frames that follow cannot get decoded. To mitigate the impact of the lost RTP video packets, Cisco Unified Border Element generates Full Intra-Frame Request (FIR) using either Real-Time Transport Control Protocol (RTCP) or SIP INFO, or both, requesting the endpoint to send a fully encoded video frame in the subsequent RTP packet.

The following types of FIR are supported on network-based recording of video calls using Cisco Unified Border Element:

- RTCP FIR (based on [RFC 5104](#)).
- SIP INFO FIR (based on [RFC 5168](#)).
- Both RTCP FIR and SIP INFO FIR (Cisco Unified Border Element can be configured to send both RTCP FIR and SIP INFO requests at the same time).

Configure Video Forking

Enabling FIR for Video Calls (Using RTCP or SIP INFO)

Perform this task to enable Full Intra-Frame Request (FIR) during the network-based recording of a video call using Real-Time Transport Control Protocol (RTCP) or using the Session Initiation Protocol (SIP) INFO method.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile video** *media-profile-tag*
4. Do one of the following:
 - **ref-frame-req rtcp** *retransmit-count* *retransmit-number*
 - **ref-frame-req sip-info**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile video <i>media-profile-tag</i> Example: Device(config)# media profile video 1	Configures a video media profile and enters media profile configuration mode.
Step 4	Do one of the following: <ul style="list-style-type: none"> • ref-frame-req rtcp retransmit-count <i>retransmit-number</i> • ref-frame-req sip-info Example: Device(cfg-mediaprofile)# ref-frame-req rtcp retransmit-count 4 Example: Device(cfg-mediaprofile)# ref-frame-req sip-info	Enables FIR using the RTCP or SIP INFO method.
Step 5	end Example: Device(cfg-mediaprofile)# end	Exits media profile configuration mode.

Configuring H.264 Packetization Mode

When a device configured as CUBE is offered more than one H.264 packetization mode on an inbound video call leg, the device offers all received modes to the outbound call leg, allowing dynamic change of mode during a call. However when a call is forked, the MediaSense recording server is not able to support this dynamic change of the packetization mode.

This feature restricts the device and allows it to offer only the configured packetization mode to the outbound call leg when media forking is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile video *media-profile-tag***
4. **h264-packetization-mode *packetization mode***
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile video <i>media-profile-tag</i> Example: Device(config)# media profile video 1	Configures a video media profile and enters media profile configuration mode.
Step 4	h264-packetization-mode <i>packetization mode</i> Example: Device(cfg-mediaprofile)# h264-packetization-mode 2	Configures the H.264 packetization mode offered by a device on the outbound call leg of a forked call when multiple H.264 packetization modes are present in the offer received by the device on the inbound call leg.
Step 5	end Example: Device(cfg-mediaprofile)# end	Exits media profile configuration mode.

Monitoring Reference files or Intra Frames

Perform this task to configure device to perform deep packet inspection (DPI) of RTP packets received from an endpoint and keep track of how many instantaneous decoder refresh (IDR) frames have been received and the timestamp of the IDRs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile video** *media-profile-tag*
4. **monitor-ref-frames**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile video media-profile-tag Example: Device(config)# media profile video 1	Configures a video media profile and enters media profile configuration mode.
Step 4	monitor-ref-frames Example: Device(cfg-mediaprofile)# monitor-ref-frames	Monitors reference frames or intra-frames.
Step 5	end Example: Device(cfg-mediaprofile)# end	Exits media profile configuration mode.

Verify for Video Forking

Perform this task to verify the additional configurations of the video recording. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show call active video called-number number | include VideoRtcpIntraFrameRequestCount**
3. **show call active video called-number number | include VideoSipInfoIntraFrameRequestCount**
4. **show call active video | include VideoTimeOfLastReferenceFrame**
5. **show call active video | include VideoReferenceFrameCount**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show call active video called-number number | include VideoRtcpIntraFrameRequestCount

Displays the number of RTCP FIR requests sent on each leg.

Example:

```
Device# show call active video called-number 990057 | include VideoRtcpIntraFrameRequestCount

! Main call legs
```

```
VideoRtcpIntraFrameRequestCount=1
VideoRtcpIntraFrameRequestCount=1

!CUBE does not generate FIR request on forked leg
VideoRtcpIntraFrameRequestCount=0
```

Step 3 **show call active video called-number *number* | include VideoSipInfoIntraFrameRequestCount**

Displays the number of SIP INFO FIR requests sent on each leg.

Example:

```
Device# show call active video called-number 990062 | include VideoSipInfoIntraFrameRequestCount

! Main call legs
VideoSipInfoIntraFrameRequestCount=1
VideoSipInfoIntraFrameRequestCount=1

!CUBE does not generate FIR request on forked leg
VideoSipInfoIntraFrameRequestCount=0
```

Step 4 **show call active video | include VideoTimeOfLastReferenceFrame**

Displays the timestamp of latest IDR frame.

Step 5 **show call active video | include VideoReferenceFrameCount**

Displays the number of IDR frames received on that call leg.



CHAPTER 54

Third-Party GUID Capture

- [Overview, on page 537](#)
- [Restrictions for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording, on page 538](#)
- [Configure Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording, on page 538](#)
- [Verify Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording, on page 541](#)
- [Configuration Examples for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording, on page 542](#)

Overview

The Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording feature provides support for the transmission of globally unique identifiers (GUIDs) received from a third-party private branch exchange (PBX) to the recording server using an established Session Initiation Protocol (SIP) session, making Cisco Unified Border Element (CUBE) recording more interoperable with third-party vendors.

Enterprise call control systems such as the Cisco Unified Communications Manager (CUCM) use globally unique identifiers (GUIDs) to correlate the multiple call legs of a single call. The call can then be forwarded or transferred, creating additional call legs associated with the same GUID. When recording is configured, CUBE initiates a SIP session with a recorder server and forks the media packets it receives or transmits, along with participant information like called number, calling number, Remote Party ID (RPID), and P-Asserted-Identity (PAI).

While the Cisco-Guid header (used by CUCM) is transmitted to the recording server, third-party GUIDs are not. Third-party GUIDs can be received through an INVITE message or a 200 OK message, depending on whether the third-party PBX is initiating the call [caller] or receiving the call [callee].

Forwarding the GUID to the recording server enables correlation between call records of the PBX and the recording server.

Feature Information

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 75: Feature Information for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording

Feature Name	Releases	Feature Information
Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording	Baseline Functionality	The Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording feature provides support for the transmission of globally unique identifiers (GUIDs) received from a third-party private branch exchange (PBX) to the recording server via an established SIP session, making CUBE recording more interoperable with third-party vendors.

Restrictions for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording

- The third-party GUID must be received through an INVITE message or a 200 OK message (depending on whether the third-party PBX is initiating the call [caller] or receiving the call [callee]). No other request type, including re-invites, is supported.
- The third-party GUID can be received only through the primary inbound call leg or the primary outbound call leg.

Cofigure Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording

To capture the third-party GUID and forward it to the recording server, you need to copy a third-party GUID header that CUBE receives, configure a SIP copylist for that header, and apply it to the primary inbound and outbound call leg dial peers. A SIP profile is configured to copy this incoming header to a user-defined variable and apply it to an outgoing header on the recording leg dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-copylist tag**
4. **sip-header *ThirdParty-GUID-headername***
5. **exit**
6. **dial-peer voice *inbound-dialpeer-tag* voip**
7. **voice class sip-copylist tag**
8. **exit**
9. **dial-peer voice *outbound-dialpeer-tag* voip**
10. **voice class sip-copylist tag**

11. **exit**
12. **voice class sip-profiles** *profile-id*
13. **request INVITE peer-header sip** *GUID-header-to-copy* **copy** *header-value-to-match* *copy-variable*
14. **request INVITE sip-header** *header-to-add* **add** *header-value-to-add*
15. **request INVITE sip-header** *GUID-header-to-modify* **modify** *header-value-to-match* *header-value-to-replace*
16. **exit**
17. **dial-peer voice** *recorder-dial-peer-tag* **voip**
18. **voice-class sip** *profiles* *profile-tag*
19. **end**

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	voice class sip-copylist <i>tag</i> Example: Device(config)# voice class sip-copylist 100	Configures a list of entities to be sent to a peer call leg and enters voice class configuration mode.
Step 4	sip-header <i>ThirdParty-GUID-headername</i> Example: Device(config-class)# sip-header Third-Party-GUID	Specifies that the third-party GUID header must be copied from the inbound dial-peer leg to the outbound dial-peer call leg.
Step 5	exit Example: Device(config-class)# exit	Exits voice class configuration mode.
Step 6	dial-peer voice <i>inbound-dialpeer-tag</i> voip Example: Device(config)# dial-peer voice 2 voip	Enters inbound dial-peer configuration mode.
Step 7	voice class sip-copylist <i>tag</i> Example: Device(config-dial-peer)# voice class sip-copylist 100	Applies the copy list to the dial peer.

	Command or Action	Purpose
Step 8	exit Example: Device(config-dial-peer)# exit	Exits to global configuration mode.
Step 9	dial-peer voice <i>outbound-dialpeer-tag</i> voip Example: Device(config)# dial-peer voice 3 voip	Enters outbound dial-peer configuration mode.
Step 10	voice class sip-copylist <i>tag</i> Example: Device(config-dial-peer)# voice class sip-copylist 100	Applies the copy list to the dial peer.
Step 11	exit Example: Device(config-dial-peer)# exit	Exits to global configuration mode.
Step 12	voice class sip-profiles <i>profile-id</i> Example: Device(config)# voice class sip-profiles 10	Creates a SIP profile and enters voice class configuration mode.
Step 13	request INVITE peer-header sip <i>GUID-header-to-copy</i> copy <i>header-value-to-match</i> <i>copy-variable</i> Example: Device(config-class)# request INVITE peer-header sip Third-Party-GUID copy "(.*)" u01	Copies headers from the INVITE message of the incoming dial peer into a copy variable.
Step 14	request INVITE sip-header <i>header-to-add</i> add <i>header-value-to-add</i> Example: Device(config-class)# request INVITE sip-header Unsupported add "Unsupported: Dummy Header"	Adds a SIP header to a SIP request.
Step 15	request INVITE sip-header <i>GUID-header-to-modify</i> modify <i>header-value-to-match</i> <i>header-value-to-replace</i> Example: Device(config-class)# request INVITE sip-header Unsupported modify ".*" "Third-Party-GUID: \u01"	Modifies the outgoing header using the copy variable defined in the previous step.
Step 16	exit Example: Device(config-class)# exit	Exits to global configuration mode.

	Command or Action	Purpose
Step 17	dial-peer voice <i>recorder-dial-peer-tag</i> voip Example: Device(config)# dial-peer voice 2 voip	Enters the dial peer configuration mode for the specified outbound recorder dial peer.
Step 18	voice-class sip profiles <i>profile-tag</i> Example: Device(config-dial-peer)# voice-class sip profiles 30	Applies the SIP profile to the recording dial peer.
Step 19	end Example: Device(config-dial-peer)# end	Exits to privileged EXEC mode.

Verify Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording

SUMMARY STEPS

1. **debug ccsp** messages for an INVITE message
2. **debug ccsp** messages for a 200 OK message

DETAILED STEPS

Step 1 **debug ccsp** messages for an INVITE message

Displays all Session Initiation Protocol (SIP) Service Provider Interface (SPI) messages for an INVITE message.

Example:

```
Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.44.29.32:5060;branch=z9hG4bK121F62
From: "sipp" <sip:1111000010@9.44.29.32>;tag=906F9C-21B9
To: "sut" <sip:4321@9.0.0.120>;tag=30050SIPpTag0111
Call-ID: 67B65D26-473711E3-8029B214-265DCDFE@9.44.29.32
CSeq: 101 INVITE
Contact: <sip:9.0.0.120:6019;transport=UDP>
Cisco-Guid: passthru
Content-Type: application/sdp
Content-Length: 108
```

Step 2 **debug ccsp** messages for a 200 OK message

Displays all Session Initiation Protocol (SIP) Service Provider Interface (SPI) messages for a 200 OK message.

Example:

```

Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.44.29.32:5060;branch=z9hG4bK121F62
From: "sipp " <sip:1111000010@9.44.29.32>;tag=906F9C-21B9
To: "sut" <sip:4321@9.0.0.120>;tag=30050SIPpTag0111
Call-ID: 67B65D26-473711E3-8029B214-265DCDFE@9.44.29.32
CSeq: 101 INVITE
Contact: <sip:9.0.0.120:6019;transport=UDP>
Cisco-Guid: passthru
Content-Type: application/sdp
Content-Length: 108

```

Configuration Examples for Third-Party GUID Capture for Correlation Between Calls and SIP-based Recording

```

! Create a copylist
Device(config)# voice class sip-copylist 100
! GUID for third party PBX
Device(config-class)# sip-header Third-Party-GUID
!GUID for CUCM
Device(config-class)# sip-header Cisco-Guid
Device(config-class)# exit

! Apply copylist to inbound dial peer so that headers specified in copylist are copied
Device(config)# dialpeer voice 2 voip
Device(config-dial-peer)# voice class sip-copylist 100
Device(config-dial-peer)# exit

! SIP profile copies incoming third-party GUID to a variable from a peer header. This
variable
! is then used modify outgoing headers
Device(config)# voice class sip-profiles 10
Device(config-class)# request INVITE peer-header sip Third-Party-GUID copy "(*)" u01
Device(config-class)# request INVITE sip-header Unsupported add "Unsupported: Dummy Header"
Device(config-class)# request INVITE sip-header Unsupported modify ".*" "Third-Party-GUID:
  \u01"
Device(config-class)# exit

! Apply SIP profile to outbound dial peer
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# voice-class sip profiles 30

```




CHAPTER 55

Network based Recording

- [Overview, on page 543](#)
- [Restrictions, on page 546](#)
- [Configure UC Gateway Services, on page 551](#)
- [Example: Configuring UC Gateway Services, on page 557](#)

Overview

The Cisco Unified Communications (UC) Services API provides a unified web service interface for the different services in IOS gateway thereby facilitating rapid service development at application servers and managed application service providers.

This chapter explains the Extended Media Forking (XMF) provider that allows applications to monitor calls and trigger media forking on Real-time Transport Protocol (RTP) and Secure RTP calls.

Feature Information

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
Cisco Unified Communications Gateway Services	Baseline Functionality	The Cisco Unified Communications (UC) Services API provides a unified web service interface for the different services in IOS gateway thereby facilitating rapid service development at application servers and managed application service providers.

Extended Media Forking (XMF) Provider and XMF Connection

The XMF provider allows applications to monitor calls and trigger media forking on the calls and has the capability to service up to 32 applications. The XMF provider can invoke a call-based or a connection-based

media forking using the Unified Communications (UC) API. After the media forking is invoked, it can preserve the media forking initiated by the web application if the WAN connection to the application is lost. The XMF provider also provides the recording tone to the parties involved in the call.

The XMF connection describes the relationship between an XMF call and the endpoint (or trunk) involved in the call. A connection abstraction maintained in the gateway has the following connection states:

- **IDLE:** This state is the initial state for all new connections. Such connections are not actively part of a telephone call, yet their references to the Call and Address objects are valid. Connections typically do not stay in the IDLE state for long and quickly transition to other states. The application may choose to be notified at this state using the event filters and if done, call/connection at the gateway provider will use the `NotifyXmfConnectionData(CREATED)` message to notify the application listener that a new connection is created.
- **ADDRESS_COLLECT:** In this state the initial information package is collected from the originating party and is examined according to the “dialing plan” to determine the end of collection of addressing information. In this state, the call in the gateway collects digits from the endpoint. No notification is provided.
- **CALL_DELIVERY:** On the originating side, this state involves selecting of the route as well as sending an indication of the desire to set up a call to the specified called party. On the terminating side, this state involves checking the busy/idle status of the terminating access and also informing the terminating message of an incoming call. The application may choose to be notified at this state using the event filters and if done, the call or connection at the gateway provider will use the `NotifyXmfConnectionData (CALL_DELIVERY)` message to notify the application listener.
- **ALERTING:** This state implies that the Address is being notified of an incoming call. The application may choose to be notified at this state using the event filters and if done, the call or connection at the gateway provider will use the `NotifyXmfConnectionData (ALERTING)` message to notify the application listener.
- **CONNECTED:** This state implies that a connection and its Address is actively part of a telephone call. In common terms, two parties talking to one another are represented by two connections in the CONNECTED state. The application may choose to be notified at this state using the event filters and if done, the call or connection at the gateway provider will use the `NotifyXmfConnectionData (CONNECTED)` message to notify the application listener.
- **DISCONNECTED:** This state implies it is no longer part of the telephone call. A Connection in this state is interpreted as once previously belonging to this telephone call. The application may choose to be notified at this state using the event filters and if done, the call or connection at the gateway provider will use the `NotifyXmfConnectionData (DISCONNECTED)` message to notify the application listener.

XMF Call-Based Media Forking

In call-based media forking of the gateway, the stream from the calling party is termed as near-end stream and the stream from the called party is termed as far-end stream.

The XMF provider actively handles single media forking request per session. Any new media forking request from the external application will override or stop the current forking instance and would start a new forking instance (to the appropriate target IP address or ports).

After the media forking request is accepted, the XMF provider returns a response message and starts to fork media streams of a connection to the target forked streams. A `NotifyXmfCallData` message will be notified

to the application for the updated media forking status, that is, FORK_FAILED, FORK_STARTED, or FORK_DONE.

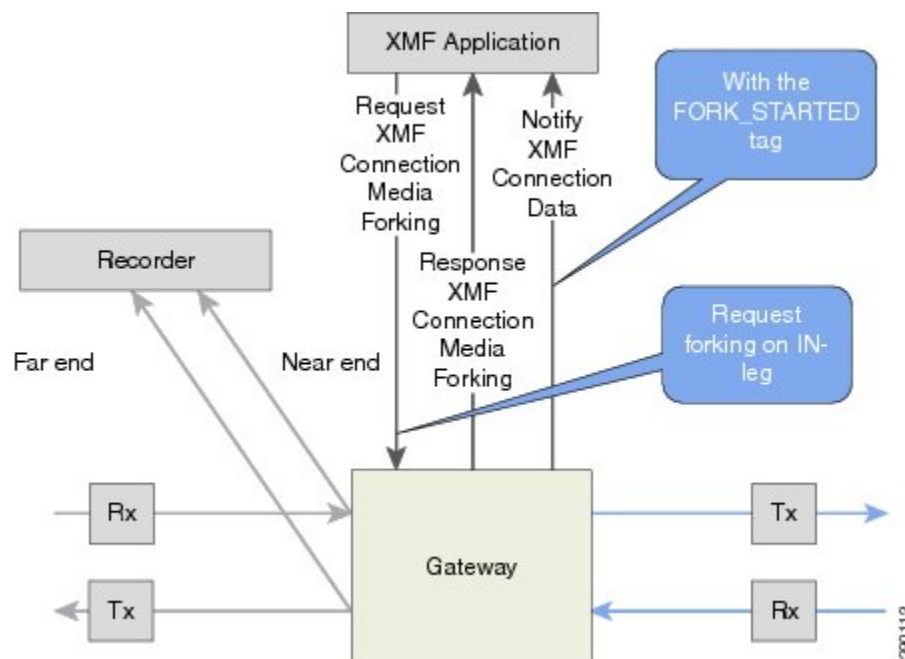
XMF Connection-Based Media Forking

In connection-based media forking of the gateway, the incoming stream to the connection is termed as near-end stream and the outgoing stream of the connection is termed as far-end stream.

The XMF provider actively handles single media forking request per session. Any new media forking request from the external application will override or stop the current forking instance and would start a new forking instance (to the appropriate target IP address or ports).

After the media forking request is accepted, the XMF provider returns a response message and starts to fork media streams of a connection to the target forked streams.

Figure 39: XMF Connection-Based Media Forking



A NotifyXmfConnectionData message will be notified to the application for the updated media forking status:

- **FORK_FAILED**—Media forking is setup failure. No forked RTP connections can be established to target RTP addresses.
- **FORK_STARTED**—Media forking is set up successfully. Both Tx (transmit) and Rx (receive) forked RTP connections are established and connected to target (farEnd and nearEnd) RTP addresses.
- **FORK_DONE**—Media forking is completed. Both Tx and Rx forked RTP connections are released.

Extended Media Forking API with Survivability TCL

Cisco Unified Border Element (CUBE) supports Survivability TCL Script to co-exist with Cisco Unified Communication (UC) Services API.

Cisco UC Services API XMF interface supports media forking for all the calls controlled by survivability TCL script including the survivability re-attempted calls. Thus, all the calls controlled by survivability TCL script can be recorded when requested by Cisco UC Services XMF API.

Cisco Unified Communications Manager controlled Gateway recording utilizes XMF to trigger media forking on CUBE or SIP based PSTN gateways in the supported call flows.



Note Media forking is allowed only for survivability TCL script supported by Cisco Unified Customer Voice Portal (CVP). CVP survivability TCL script is not supported in High Availability mode.

The following call scenarios are supported:

- Basic comprehensive call
- Calls with Refer Consume
- Calls with Mid-call failure
- Calls with alternative route with initial call failure

There are no configuration changes required for enabling CVP survivability TCL support with Cisco UC Gateway Services API.

Restrictions

The Extended Media Forking does not support the following:

- Media renegotiation.
- Media mixing on forked media streams.
- recordTone insertion with SRTP calls.
- mediaForkingReason tag is only to notify midcall stream events; notification for events such as codec change.
- Supplementary services such as hold/resume, call forward, call transfer, and so on.
- High Availability (HA).
- Virtual Routing and Forwarding (VRF) or Multi-VRF.
- Hair-pinning calls from CUBE to Cisco Unified Customer Voice Portal (CVP) and back to the same CUBE for Extended Media Forking (XMF) Gateway recording.
- Forking of calls on a TDM leg.



Note • Only voice media stream is supported.

Example of SDP Data sent in an SRTP Call

Original SIP SDP Crypto Offer	SIP SDP Crypto Answer
v=0	v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98	o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call	s=SIP Call
c=IN IP4 172.18.193.98	c=IN IP4 172.18.193.98
t= 0 0	t=0 0
m=audio 51372 RTP/SAVP 0	m=audio 49170 RTP/SAVP 0
a=rtpmap:0 PCMU/8000	a=crypto:1 AES_CM_128_HMAW_SHA1_32
a=crypto:1 AES_CM_128_HMAC_SHA1_32	inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpXlZj
inline:0RmdmcmVCspEc3QGZINWpVLEJhQX1cfHawJSoj	



Note The application is notified of the content in Crypto and inline SDP lines.

Crypto Tag

For SRTP forking, the optional Crypto tag in NotifyXmfConnectionData or NotifyXmfCallData message indicates the context of an actively forked SRTP connection.



Note The Crypto tag is only present in the notification message where FORK_STARTED tag is present.

The optional Crypto tag specifies the following:

- The Crypto suite used for encryption and authentication algorithm.
- The base64 encoded primary key and salt used for encryption.

Crypto suite can be one of the two suites supported in IOS:

- AES_CM_128_HMAC_SHA1_32
- AES_CM_128_HMAC_SHA1_80

Example of SDP Data sent in an SRTP Call

Original SIP SDP Crypto Offer	SIP SDP Crypto Answer
<pre>v=0 o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98 s=SIP Call c=IN IP4 172.18.193.98 t= 0 0 m=audio 51372 RTP/SAVP 0 a=rtpmap:0 PCMU/8000 a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:0RmndmcmVCspEc3QGZINWpVLFJhQX1dHAwJSoj</pre>	<pre>v=0 o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98 s=SIP Call c=IN IP4 172.18.193.98 t=0 0 m=audio 49170 RTP/SAVP 0 a=crypto:1 AES_CM_128_HMAW_SHA1_32 inline:NzB4d1BINUAvLEw6UzF3WSI+PSdFcGdUJShpX1Zj</pre>



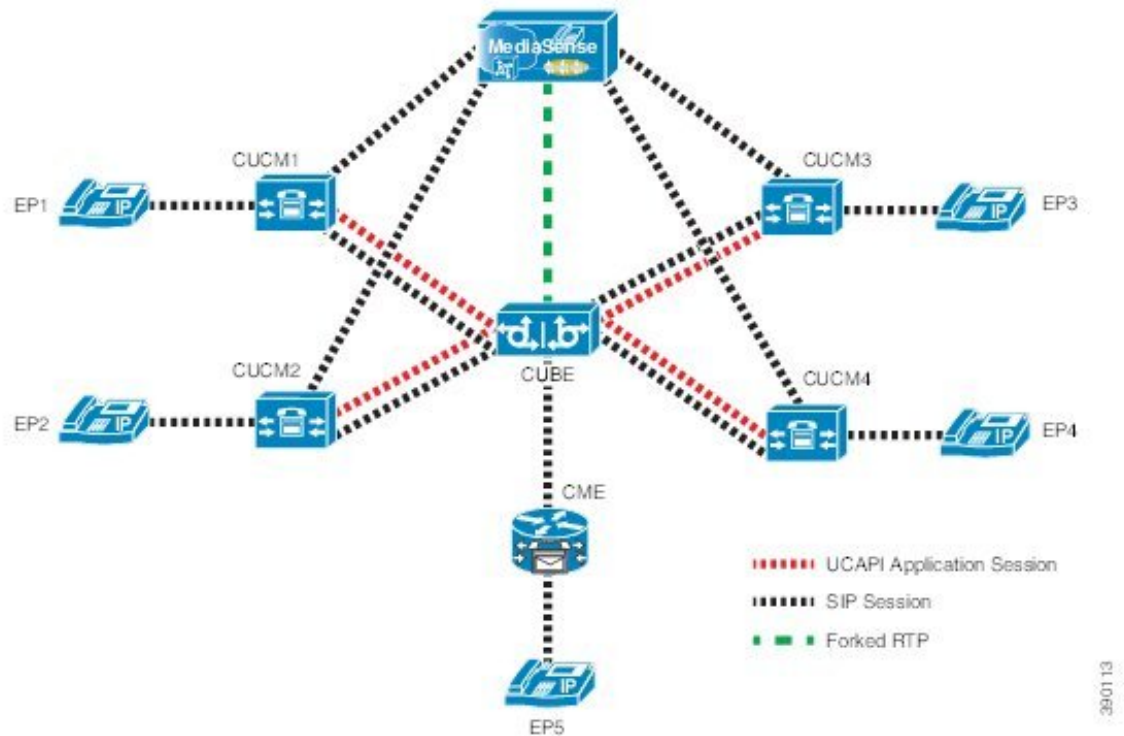
Note The application is notified of the content in Crypto and inline SDP lines.

Multiple XMF Applications and Recording Tone

Multiple XMF allows multiple (maximum 32) web applications to register with the XMF provider as separate XMF applications and provide redundancy for the voice calls recording. Recording tone provides recording tone capability to the recording sessions. Recording tone is supported for IP to IP, IP to TDM, and TDM to TDM trunks.

An example topology is as shown below where 4 CUCM applications are deployed. CUCM triggers media forking request to CUBE. Recording tone is played to the parties involved in the call based on the recordTone parameter set in the media forking request.

Figure 40: Multiple XMF Applications and Recording Tone



Media forking can be invoked using any of the following APIs:

- RequestXmfConnectionMediaForking
- RequestXmfCallMediaForking
- RequestXmfCallMediaSetAttributes

The “recordTone” parameter can be enabled in any of the above requests and recording tone will be played for the parties involved in the call. The “recordTone” parameter in the API request can have the following values:

- COUNTRY_US
- COUNTRY_AUSTRALIA
- COUNTRY_GERMANY
- COUNTRY_RUSSIA
- COUNTRY_SPAIN
- COUNTRY_SWITZERLAND

There is no difference in the recording tone beep when any country value is chosen. Recording tone beep is played at an interval of every 15 seconds. Digital signal processors and other resources are not utilized for playing recording tone even for transcoded calls. No specific configuration is required to enable or disable recording tone. By default, no recording tone is enabled.

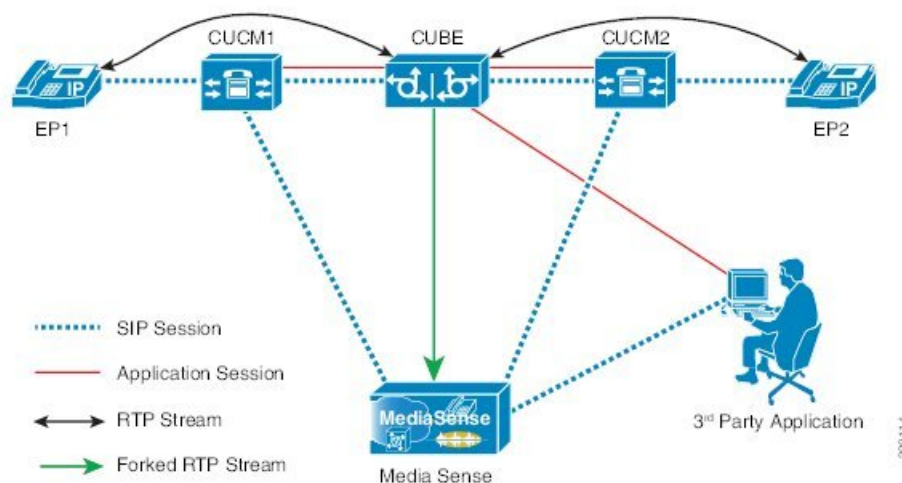
If “recordTone” parameter is enabled only on the farEndAddr, then this tone is played only on the outgoing leg. Likewise, if enabled only on the nearEndAddr, then the tone is played only on the incoming leg. When enabled in both the far and near end, then recording tone is played on both the legs.

The RequestXmfConnectionMediaForking API allows insertion of recording tone on a per connection basis. There could be scenarios where one leg receives two recordTone insertion requests. When a leg receives recordTone insertion request, the nearEnd request always takes precedence over the farEnd request.

Forking Preservation

After media forking is initiated by the web application, the forking can be preserved to continue the recording, even if the WAN connection to the application is lost or if the application is unregistered.

Figure 41: Forking Preservation



The “preserve” parameter value can be set to TRUE or FALSE in any of the 3 forking requests (RequestXmfConnectionMediaForking, RequestXmfCallMediaForking, or RequestXmfCallMediaSetAttributes) from the application to CUBE.

- If the “preserve” parameter received is TRUE, then forking will continue the recording, even if the WAN connection to application is lost or application is unregistered.
- If the “preserve” parameter received is FALSE, then forking will not continue the recording.
- If the “preserve” parameter is not received in the media forking request, then forking will not continue the recording.

Configure UC Gateway Services

Configure Cisco Unified Communication IOS Services on the Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http max-connections** *value*
5. **ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*
6. **http client connection idle timeout** *seconds*
7. **uc wsapi**
8. **message-exchange max-failures** *number*
9. **probing max-failures** *number*
10. **probing interval keepalive** *seconds*
11. **probing interval negative** *seconds*
12. **source-address** *ip-address*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip http server Example: Device(config)# ip http server	Enables the HTTP server (web server) on the system.
Step 4	ip http max-connections <i>value</i> Example: Device(config)# ip http max-connection 100	Sets the maximum number of concurrent connections to the HTTP sever that will be allowed. The default value is 5.

	Command or Action	Purpose
Step 5	<p>ip http timeout-policy idle <i>seconds</i> life <i>seconds</i> requests <i>value</i></p> <p>Example:</p> <pre>Device(config)# ip http timeout-policy idle 600 life 86400 requests 86400</pre>	<p>Sets the characteristics that determine how long a connection to the HTTP server should remain open. The characteristics are:</p> <ul style="list-style-type: none"> • idle—The maximum number of seconds the connection will be kept open if no data is received or response data can not be sent out on the connection. Note that a new value may not take effect on any already existing connections. If the server is too busy or the limit on the life time or the number of requests is reached, the connection may be closed sooner. The default value is 180 seconds (3 minutes). • life—The maximum number of seconds the connection will be kept open, from the time the connection is established. Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the number of requests is reached, it may close the connection sooner. Also, since the server will not close the connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes. The default value is 180 seconds (3 minutes). The maximum value is 86400 seconds (24 hours). • requests—The maximum limit on the number of requests processed on a persistent connection before it is closed. Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the life time is reached, the connection may be closed before the maximum number of requests are processed. The default value is 1. The maximum value is 86400.
Step 6	<p>http client connection idle timeout <i>seconds</i></p> <p>Example:</p> <pre>Device(config)# http client connection idle timeout 600</pre>	<p>Sets the number of seconds that the client waits in the idle state until it closes the connection.</p>
Step 7	<p>uc wsapi</p> <p>Example:</p> <pre>Device(config)# uc wsapi</pre>	<p>Enters Cisco Unified Communication IOS Service configuration mode.</p>

	Command or Action	Purpose
Step 8	<p>message-exchange max-failures <i>number</i></p> <p>Example:</p> <pre>Device(config-uc-wsapi)# message-exchange max-failures 2</pre>	Configures the maximum number of failed message exchanges between the application and the provider before the provider stops sending messages to the application. Range is 1 to 3. Default is 1.
Step 9	<p>probing max-failures <i>number</i></p> <p>Example:</p> <pre>Device(config-uc-wsapi)# probing max-failures 5</pre>	Configures the maximum number of failed probing messages before the router unregisters the application. Range is 1 to 5. Default is 3.
Step 10	<p>probing interval keepalive <i>seconds</i></p> <p>Example:</p> <pre>Device(config-uc-wsapi)# probing interval keepalive 255</pre>	<p>Configures the time interval between probing messages when the session is in a keepalive state. Range is from 1 to 255 seconds. Default is 5 seconds.</p> <p>Note The keepalive timer restarts when a valid HTTP message is received from the UC services API. The following are valid HTTP messages that can restart the timer:</p> <ul style="list-style-type: none"> • RESPONSE_XMF_REGISTER • RESPONSE_XMF_CONN_MEDIA_FORKING • SOLICIT_XMF_PROBING • NOTIFY_XMF_CONNECTION_DATA
Step 11	<p>probing interval negative <i>seconds</i></p> <p>Example:</p> <pre>Device(config-uc-wsapi)# probing interval negative 10</pre>	Configures the interval between negative probing messages, in seconds.
Step 12	<p>source-address <i>ip-address</i></p> <p>Example:</p> <pre>Device(config-uc-wsapi)# source-address 192.1.12.14</pre>	<p>Configures the IP address (hostname) as the source IP address for the UC IOS service.</p> <p>Note The source IP address is used by the provider in the NotifyProviderStatus messages.</p>
Step 13	<p>end</p> <p>Example:</p> <pre>Device(config-uc-wsapi)# end</pre>	Returns to privileged EXEC mode.

Configure the XMF Provider

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **uc wsapi**
4. **source-address** *ip address*
5. **provider xmf**
6. **no shutdown**
7. **remote-url** *index url*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	uc wsapi Example: Device(config)# uc wsapi	Enters Cisco Unified Communication IOS Service configuration mode.
Step 4	source-address <i>ip address</i> Example: Device(config)# source-address 172.156.19.38	Configures the source ip address.
Step 5	provider xmf Example: Device(config-uc-wsapi)# provider xmf	Enters XMF provider configuration mode.
Step 6	no shutdown Example: Device(config-uc-wsapi)# no shutdown	Activates XMF provider.

	Command or Action	Purpose
Step 7	remote-url <i>index url</i> Example: Device(config-uc-wsapi)# remote-url 1 http://test.com:8090/ucm_xmf	Specifies the URL (IP address and port number) that the application uses to communicate with XMF provider. The XMF provider uses the IP address and port to authenticate incoming requests.
Step 8	end Example: Device(config-uc-wsapi)# end	Returns to privileged EXEC mode.

Verify the UC Gateway Services

The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show wsapi registration all**
3. **show wsapi registration xmf** *remote-url-index*
4. **show call media-forking**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show wsapi registration all

Displays the details of applications registered. Each registered application is identified by a different ID.

Example:

```
Device# show wsapi registration all
```

```

Provider XMF
=====
registration index: 11
  id: 2E7C3034:XMF:myapp:26
  appUrl:http://pascal-lnx.cisco.com:8094/xmf
  appName: myapp
  provUrl: http://9.45.46.16:8090/cisco_xmf
  prober state: STEADY
  connEventsFilter:
CREATED|REDIRECTED|ALERTING|CONNECTED|TRANSFERRED|CALL_DELIVERY|DISCONNECTED|HANDOFF_JOIN|HANDOFF_LEAVE

  mediaEventsFilter: DTMF|MEDIA_ACTIVITY|MODE_CHANGE|TONE_DIAL|TONE_OUT_OF_SERVICE|TONE_SECOND_DIAL

```

```

registration index: 1
  id: 2E7C304A:XMF:myapp:27
  appUrl:http://pascal-lnx.cisco.com:8092/xmf
  appName: myapp
  provUrl: http://9.45.46.16:8090/cisco_xmf
  prober state: STEADY
  connEventsFilter:
CREATED|REDIRECTED|ALERTING|CONNECTED|TRANSFERRED|CALL_DELIVERY|DISCONNECTED|HANDOFF_JOIN|HANDOFF_LEAVE

  mediaEventsFilter: DTMF|MEDIA_ACTIVITY|MODE_CHANGE|TONE_DIAL|TONE_OUT_OF_SERVICE|TONE_SECOND_DIAL

registration index: 21
  id: 2E7C6423:XMF:myapp:28
  appUrl:http://pascal-lnx.cisco.com:8096/xmf
  appName: myapp
  provUrl: http://9.45.46.16:8090/cisco_xmf
  prober state: STEADY
  connEventsFilter:
CREATED|REDIRECTED|ALERTING|CONNECTED|TRANSFERRED|CALL_DELIVERY|DISCONNECTED|HANDOFF_JOIN|HANDOFF_LEAVE

  mediaEventsFilter: DTMF|MEDIA_ACTIVITY|MODE_CHANGE|TONE_DIAL|TONE_OUT_OF_SERVICE|TONE_SECOND_DIAL

registration index: 31
  id: 2E7C69E8:XMF:myapp:29
  appUrl:http://pascal-lnx.cisco.com:8098/xmf
  appName: myapp
  provUrl: http://9.45.46.16:8090/cisco_xmf
  prober state: STEADY
  connEventsFilter:
CREATED|REDIRECTED|ALERTING|CONNECTED|TRANSFERRED|CALL_DELIVERY|DISCONNECTED|HANDOFF_JOIN|HANDOFF_LEAVE

  mediaEventsFilter: DTMF|MEDIA_ACTIVITY|MODE_CHANGE|TONE_DIAL|TONE_OUT_OF_SERVICE|TONE_SECOND_DIAL

```

Step 3 `show wsapi registration xmf remote-url-index`

Displays the details of only a particular XMF registered application with any ID ranging from 1 to 32.

Example:

```

Device# show wsapi registration xmf 1

Provider XMF
=====
registration index: 1
  id: 2E7C6423:XMF:myapp:28
  appUrl:http://pascal-lnx.cisco.com:8096/xmf
  appName: myapp
  provUrl: http://9.45.46.16:8090/cisco_xmf
  prober state: STEADY
  connEventsFilter:
CREATED|REDIRECTED|ALERTING|CONNECTED|TRANSFERRED|CALL_DELIVERY|DISCONNECTED|HANDOFF_JOIN|HANDOFF_LEAVE

  mediaEventsFilter: DTMF|MEDIA_ACTIVITY|MODE_CHANGE|TONE_DIAL|TONE_OUT_OF_SERVICE|TONE_SECOND_DIAL

```

Step 4 `show call media-forking`

Displays the forked stream information.

Example:

```

Device# show call media-forking

Warning: Output may be truncated if sessions are added/removed concurrently!

```

```

Session    Call      n/f Destination (port address)
187        BA        near 45864 10.104.105.232
188        BA        far 54922 10.104.105.232
189        B9        near 45864 10.104.105.232
190        B9        far 54922 10.104.105.232

```

FORK_DONE Notifications

```

//WSAPI/INFRA/wsapi_send_outbound_message_by_provider_info:
*Dec 21 10:31:21.016 IST: //WSAPI/INFRA/0/9/546CF8:25:tx_contextp 15898C1C tx_id 19 context1 (0 0)
context2 (9 9):
out_url http://gauss-lnx.cisco.com:8081/xmf*Dec 21 10:31:21.020 IST:
wsapi_send_outbound_message_by_provider_info:
<?xml version="1.0" encoding="UTF-8"?><SOAP:Envelope
xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope"><SOAP:Body>
<NotifyXmfConnectionData xmlns="http://www.cisco.com/schema/cisco_xmf/v1_0"><msgHeader><transactionID>
546CF8:25</transactionID><registrationID>4CA5E4:XMF:myapp:4</registrationID></msgHeader><callData><callID>25</callID><state>
ACTIVE</state></callData><connData><connID>132</connID><state>ALERTING</state></connData><event><mediaForking>
<mediaForkingState>FORK_DONE</mediaForkingState></mediaForking></event></NotifyXmfConnectionData></SOAP:Body></SOAP:Envelope>

```

FORK_FAILED Notification

```

//WSAPI/INFRA/wsapi_send_outbound_message_by_provider_info:
*Dec 21 10:31:21.016 IST: //WSAPI/INFRA/0/9/546CF8:25:tx_contextp 15898C1C tx_id 19 context1 (0 0)
context2 (9 9):
out_url http://gauss-lnx.cisco.com:8081/xmf*Dec 21 10:31:21.020 IST:
wsapi_send_outbound_message_by_provider_info:
<?xml version="1.0" encoding="UTF-8"?><SOAP:Envelope
xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope"><SOAP:Body>
<NotifyXmfConnectionData xmlns="http://www.cisco.com/schema/cisco_xmf/v1_0"><msgHeader><transactionID>
546CF8:25</transactionID><registrationID>4CA5E4:XMF:myapp:4</registrationID></msgHeader><callData><callID>25</callID><state>
ACTIVE</state></callData><connData><connID>132</connID><state>ALERTING</state></connData><event><mediaForking>
<mediaForkingState>FORK_FAILED</mediaForkingState></mediaForking></event></NotifyXmfConnectionData></SOAP:Body>
</SOAP:Envelope>

```

Tips to Troubleshoot

Use the following **debug** commands to troubleshoot the UC Gateway Services configurations.

- **debug wsapi infrastructure all**
- **debug wsapi xmf all**
- **debug wsapi xmf messages**
- **debug wsapi infrastructure detail**
- **debug voip application**
- **debug voip application media forking**

Example: Configuring UC Gateway Services

```

uc wsapi
message-exchange max-failures 5

```

```

response-timeout 10
source-address 192.1.12.14
probing interval negative 20
probing interval keepalive 250
!
provider xmf
remote-url 1 http://pascal-lnx.cisco.com:8050/ucm_xmf

```

Example: Configuring Cisco Unified Communication IOS Services

The following example shows how to configure the device for Cisco Unified Communication IOS Services and enable the HTTP server:

```

Device> enable
Device# configure terminal
Device(config)# ip http server
Device(config)# ip http max-connection 100
Device(config)# ip http timeout-policy idle 600 life 86400 requests 86400
Device(config)# http client connection idle timeout 600
Device(config)# uc wsapi
Device(config-uc-wsapi)# message-exchange max-failures 2
Device(config-uc-wsapi)# probing max-failures 5
Device(config-uc-wsapi)# probing interval keepalive 255
Device(config-uc-wsapi)# probing interval negative 10
Device(config-uc-wsapi)# source-address 192.1.12.14
Device(config-uc-wsapi)# end

```

Example: Configuring the XMF Provider

The following example shows how to enable the XMF providers. The configuration specifies the address and port that the application uses to communicate with the XMF provider:

```

Device> enable
Device# configure terminal
Device(config)# uc wsapi
Device(config-uc-wsapi)# provider xmf
Device(config-uc-wsapi)# no shutdown
Device(config-uc-wsapi)# remote-url 1 http://test.com:8090/ucm_xmf
Device(config-uc-wsapi)# end

```

Example: Configuring UC Gateway Services

```

uc wsapi
message-exchange max-failures 5
response-timeout 10
source-address 192.1.12.14
probing interval negative 20
probing interval keepalive 250
!
provider xmf
remote-url 1 http://pascal-lnx.cisco.com:8050/ucm_xmf

```




CHAPTER 56

Media Proxy and Recording

- Overview, on page 559
- Supported Platforms, on page 560
- Restrictions, on page 560
- CUBE Media Proxy Using Unified CM Network-Based Recording, on page 561
- SIPREC-Based Media Proxy, on page 561
- About Multiple Media Forking Using CUBE Media Proxy, on page 561
- Deployment Scenarios for Media Proxy, on page 562
- Media Proxy Configuration, on page 572
- Verification of CUBE Media Proxy Configuration, on page 578
- Supported Features, on page 588

Overview

Cisco Unified Border Element (CUBE) Media Proxy is a solution that provides multiple forking function, and is built on CUBE architecture. Multiple forks are required for recorder redundancy and advanced media processing needs. The CUBE Media Proxy solution supports mandatory and optional recorders.

CUBE Media Proxy supports Unified CM Network-Based Recording (NBR) and SIP-Based Media Recording (SIPREC), to enable forking and recording of Real-Time Transport Protocol (RTP) streams.

Feature Information

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 76: Feature Information for Recording Proxy

Feature Name	Releases	Feature Information
Secure forking of nonsecure calls	Cisco IOS XE Bengaluru 17.5.1a	CUBE Media Proxy supports both secure and nonsecure forking of nonsecure calls.

Feature Name	Releases	Feature Information
SIPREC-Based CUBE Media Proxy	Cisco IOS XE Amsterdam 17.3.1a	The SIPREC-based CUBE Media Proxy solution supports forking to multiple recorders.
CUBE Media Proxy	IOS XE Gibraltar Release 16.10.1a	The CUBE Media Proxy solution provides multiple forking functions for redundancy and advanced media processing.

Supported Platforms

CUBE Media Proxy is supported on the following Cisco router platforms running on Cisco IOS XE Software Releases:

- Cisco 4000 Series-Integrated Services Routers (ISR4321, ISR4331, ISR4351, ISR4431, ISR4451, and ISR4461)
- Cisco Aggregated Services Routers (ASR - ASR1001-X, ASR1002-X, ASR1004 with RP2, ASR1006 with RP2, Cisco ASR1006-X Aggregated Services Routers with RP2 and ESP40, ASR 1006-X with RP3 and ESP40/ESP100)
- Cisco Cloud Services Routers (CSR1000V series)
- Cisco Catalyst 8000V Edge Software (Catalyst 8000V) series
- Cisco 8300 Catalyst Edge Series Platforms (C8300-1N1S-6T, C8300-2N2S-6T, C8300-1N1S-4T2X, C8300-2N2S-4T2X)
- Cisco 8200 Catalyst Edge Series Platform (C8200-1N-4T)
- Cisco 8200L Catalyst Edge Series Platform (C8200L-1N-4T)



Note When upgrading to C8000V software from a CSR1000V release, an existing throughput configuration will be reset to a maximum of 250Mbps. Install an HSEC authorization code, which you can obtain from your Smart License account, before reconfiguring your required throughput level.

Restrictions

CUBE Media Proxy using Unified CM NBR, and SIPREC-Based CUBE Media Proxy do not support the following:

- Forking of video sessions
- Recording of calls from endpoints that are registered with the Cloud. For example, Cisco Webex Calling.
- SRTP fallback
- Midcall block
- Concurrent use with CUBE B2BUA SBC features.

- Server Groups in outbound dial-peers toward recorders.
- Midcall updates from the recorders such as pause or resume recording, RE-INVITE with SDP changes, INVITE that replaces header that is sent by recorders when they switch from active to standby CUBE Media Proxy.



Note Midcall update "BYE" from the recorders is supported.

- Unified CM NBR and SIPREC for the same call flow.

The following restriction applies when using CUBE Media Proxy with Unified CM NBR:

- If the primary recorder sends a=inactive in the response SDP, the same is forwarded to Unified CM. Forking is not triggered to any of the recorders.

CUBE Media Proxy Using Unified CM Network-Based Recording

CUBE Media Proxy using Unified CM Network-Based Recording (NBR), is Unified CM dependent and requires you to configure inbound dial-peers from Unified CM. After receiving a media forking request from Unified CM, the CUBE Media Proxy establishes media forks to the configured targets.

SIPREC-Based Media Proxy

The SIPREC (SIP Media Recording) feature supports media recording for Real-Time Transport Protocol (RTP) streams in compliance with section 3.1.1. of RFC 7245, with CUBE Media Proxy acting as the Session Recording Client (SRC). SIP is used to establish a Recording Session between the CUBE Media Proxy and recorders (or any other media application).

For SIPREC solutions, CUBE Media Proxy accepts an inbound RTP fork from a CUBE SBC and replicates this RTP fork to multiple SIPREC targets based on its inbound configuration.

About Multiple Media Forking Using CUBE Media Proxy

Unified CM Network-Based CUBE Media Proxy and SIPREC-Based CUBE Media Proxy support the following functions:

- Media forking for up to five destinations per call
- Destination redundancy by hunting algorithm
- Media fork policy control
- Load balancing during initial call setup
- High Availability
- TLS, TCP, and UDP transport protocols
- Secure forking of nonsecure calls

- Secure forking of secure calls

Secure Forking of Secure and Nonsecure Calls

From Cisco IOS XE Bengaluru 17.5.1a onwards, you can configure a combination of secure and nonsecure forks for a nonsecure call.

[CUBE Media Proxy Using Unified CM Network-Based Recording, on page 561](#) supports secure forking of secure and nonsecure calls.



Note You cannot use the **mandatory policy** command with secure forking configurations.

For SRTP pass through to work in secure media forking, the Command Line Interface **srtp pass-thru** should be configured at global or dial-peer level.

Deployment Scenarios for Media Proxy



Note From Cisco IOS XE Bengaluru 17.5.1a onwards, you can deploy a combination of secure and nonsecure destinations.

Media Proxy Using Unified CM Network-Based Recording

In Network Based Recording (NBR) deployments, Cisco Unified Communications Manager establishes an initial forked media leg with CUBE Media Proxy. This may either be from a phone using its built-in bridge, ([Deployment Scenario for CUBE Media Proxy Using Unified CM NBR for External Call](#)), or from a CUBE SBC using the eXtended Media Forking (XMF) API ([Deployment Scenario for CUBE Media Proxy Using Unified CM NBR for External Call](#)).

Figure 42: Deployment Scenario for CUBE Media Proxy Using Unified CM NBR for External Call

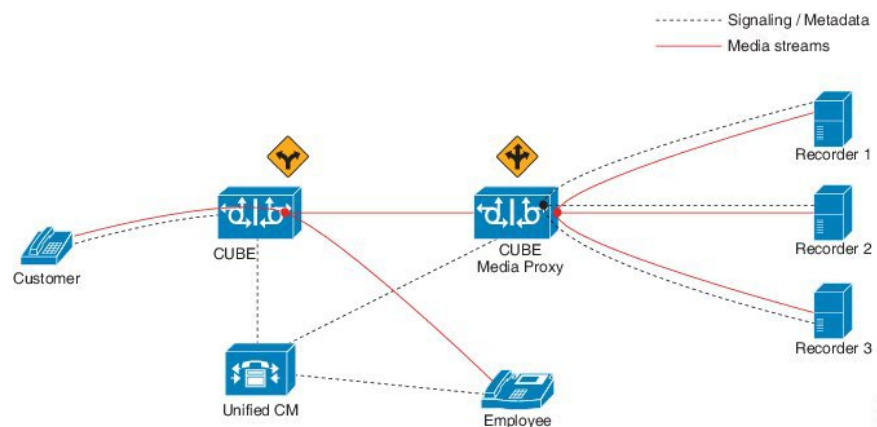
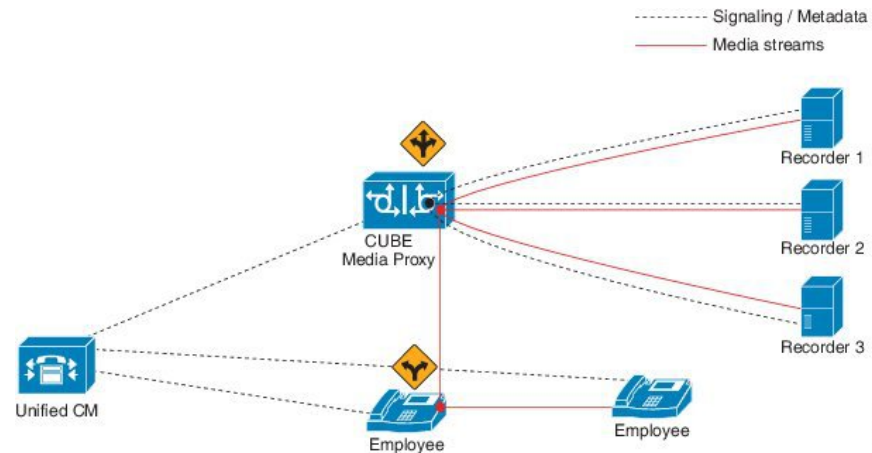


Figure 43: Deployment Scenario for CUBE Media Proxy Using Unified CM NBR for Internal Call



The information flow is as follows:

1. External or internal call is set up between the endpoints.
2. CUBE Media Proxy receives the media forking request from UCM.
3. CUBE Media Proxy sets up sessions with the recorders based on the proxy policy.
 - Mandatory recorder: Proxy policy is configured to set a recorder as mandatory. CUBE Media Proxy tries to establish connection with the mandatory recorder. Forking to the remaining recorders happen only if the connection with the mandatory recorder is successful.
 - Optional recorders: When the proxy policy is not configured, all the recorders are set as optional. CUBE Media Proxy tries to establish a connection with the remaining recorders even if any of the recorders fail.



Note

- If the CUBE Media Proxy receives a '486' response from the initial recorder, CUBE Media Proxy does not fork the INVITE to other recorders. To perform alternate routing, configure the **voice hunt user-busy** command in global configuration mode.

Example: **Router(config)# voice hunt user-busy**

- Secure recorders: When secure recorders are configured, mandatory proxy policy configuration does not apply. CUBE Media Proxy tries to establish a connection with the first secure recorder from the list of configured dial-peers. Forking to the remaining recorders happens after establishing a connection with the first secure recorder.
4. If required, Cisco Unified SIP Proxy may be used to route or load balance a media fork for a group of recorders.

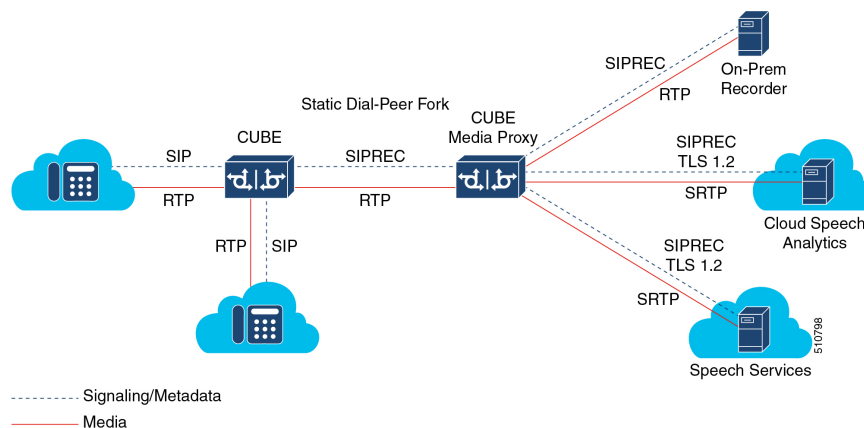


Note The CUBE Media Proxy solution supports Unified CM Release 12.5.1 and Cisco Unified SIP Proxy Release 9.1.8.

SIPREC-Based Media Proxy

CUBE Media Proxy may be configured to fork media autonomously using SIPREC, as shown in the following scenario.

Figure 44: Deployment Scenario for SIPREC-Based CUBE Media Proxy



The information flow in this scenario is as follows:

1. CUBE SBC receives a call from a SIP trunk and routed to the intended destination.
2. CUBE SBC uses SIPREC to establish a media fork of the call with CUBE Media Proxy.
3. CUBE Media Proxy uses SIPREC to establish secure or nonsecure media forks with up to five destinations.



Note On receiving BYE from the primary secure recorder, Media Proxy disconnects all secure and nonsecure recording sessions. BYE received from any other recorder, secure or nonsecure, will not impact other active recording sessions.

Recording Metadata

Metadata is the information that a Recording Server (RS) receives from a Recording Client (RC) in a SIP session. Metadata has the following functions:

- Carries the communication session data that describes the call to the Recording Server.
- Identifies the participants list.
- Identifies the session and media association time.

Recording Metadata in CUBE Media Proxy Using Unified CM NBR

Unified CM passes information about the forked call to CUBE Media Proxy in up to 16 metadata parameters that are included in the From header of the SIP Invite. CUBE Media Proxy includes a copy of this metadata in the Invite it sends to the configured destinations. The following is an example of a **From** header with metadata.



Note The **From** header, including all metadata must not exceed 583 bytes.

Following is a sample SIP header of a recording request:

```
From: "abcd" <sip:198101@10.200.25.137;
x-nearend;x-refci=27298698;x-nearendclusterid=NY-NJ-Labcluster;
x-nearenddevice=SEP2834A28318CE;
x-nearendaddr=198101;x-farendrefci=27298699;
x-farendclusterid=NY-NJ-Labcluster;x-farenddevice=AFIFIM-VI1;x-farendaddr=172001;
x-sessionid=696dd5d3f7755c6abdc438e93d01febf>;
tag=14087~b35a5915-3167-4d6a-871d-c121221602bf-27298703
```

Recording Metadata in SIPREC-Based CUBE Media Proxy

The initial SIPREC Invite from CUBE to CUBE Media Proxy, and the SIPREC Invite from CUBE Media Proxy to the recorders, includes recording metadata in a SIPREC XML body.

Following is a sample SIPREC INVITE:

```
INVITE sip:9876@8.43.33.203:5060 SIP/2.0
Via: SIP/2.0/UDP 8.43.33.209:5060;branch=z9hG4bK20959B
From: <sip:8.43.33.209>;tag=678813-6AC
To: <sip:9876@8.43.33.203>
Date: Thu, 13 Feb 2020 03:35:19 GMT
Call-ID: B0FA2851-4D4811EA-82E5D263-E98F8024@8.43.33.209
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Require: siprec
Min-SE: 1800
Cisco-Guid: 2967454021-1296568810-2195116643-3918495780
User-Agent: Cisco-SIPGateway/IOS-17.3.20200207.160928
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1581564919
Contact: <sip:8.43.33.209:5060>;+sip.src
Expires: 180
Allow-Events: telephone-event
Session-ID: 812eae44f57c50b38e897d75d8e12809;remote=00000000000000000000000000000000
Content-Type: multipart/mixed;boundary=uniqueBoundary
Mime-Version: 1.0
Content-Length: 2250

--uniqueBoundary
Content-Type: application/sdp
Content-Disposition: session;handling=required

v=0
o=CiscoSystemsSIP-GW-UserAgent 5146 1045 IN IP4 8.43.33.209
```

```

s=SIP Call
c=IN IP4 8.43.33.209
t=0 0
m=audio 8278 RTP/AVP 0
c=IN IP4 8.43.33.209
a=rtpmap:0 PCMU/8000
a=ptime:20
a=sendonly
a=label:1
m=audio 8280 RTP/AVP 0
c=IN IP4 8.43.33.209
a=rtpmap:0 PCMU/8000
a=ptime:20
a=sendonly
a=label:2

--uniqueBoundary
Content-Type: application/rs-metadata+xml
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns="urn:ietf:params:xml:ns:recording:1">
  <datamode>complete</datamode>
  <session session_id="sPVtz01IEeqC3dJj6Y+AJA==">
    <sipSessionID>0e0960d88013509f86e7ad2d78da208a;remote=4d0de1325c205fa08f77d8d31c1b3a6f</sipSessionID>

      <start-time>2020-02-13T03:35:19.008Z</start-time>
    </session>
    <participant participant_id="sPVtz01IEeqC3tJj6Y+AJA==">
      <nameID aor="sip:3478@8.41.17.71">
        </nameID>
      </participant>
      <participantsessionassoc participant_id="sPVtz01IEeqC3tJj6Y+AJA=="
session_id="sPVtz01IEeqC3dJj6Y+AJA==">
        <associate-time>2020-02-13T03:35:19.008Z</associate-time>
      </participantsessionassoc>
      <stream stream_id="sPgFxxk1IEeqC49Jj6Y+AJA==" session_id="sPVtz01IEeqC3dJj6Y+AJA==">
        <label>1</label>
      </stream>
      <participant participant_id="sPVtz01IEeqC39Jj6Y+AJA==">
        <nameID aor="sip:98765@8.41.17.71">
          </nameID>
        </participant>
        <participantsessionassoc participant_id="sPVtz01IEeqC39Jj6Y+AJA=="
session_id="sPVtz01IEeqC3dJj6Y+AJA==">
          <associate-time>2020-02-13T03:35:19.008Z</associate-time>
        </participantsessionassoc>
        <stream stream_id="sPgFxxk1IEeqC5Nj6Y+AJA==" session_id="sPVtz01IEeqC3dJj6Y+AJA==">
          <label>2</label>
        </stream>
        <participantstreamassoc participant_id="sPVtz01IEeqC3tJj6Y+AJA==">
          <send>sPgFxxk1IEeqC49Jj6Y+AJA==</send>
          <recv>sPgFxxk1IEeqC5Nj6Y+AJA==</recv>
        </participantstreamassoc>
        <participantstreamassoc participant_id="sPVtz01IEeqC39Jj6Y+AJA==">
          <send>sPgFxxk1IEeqC5Nj6Y+AJA==</send>
          <recv>sPgFxxk1IEeqC49Jj6Y+AJA==</recv>
        </participantstreamassoc>
      </recording>

--uniqueBoundary--

```


For a SIPREC call, the Require header in the SIP Invite (from CUBE to CUBE Media Proxy, and from CUBE Media Proxy to the recorders) must have a "siprec" extension. The Require header must also have metadata in the XML body, else, the call is dropped. The Contact header in a SIP invite has a "+sip.src" extension.

Session Identifier

In both NBR and SIPREC modes, CUBE Media Proxy uses the Session-ID header in request and response messages to exchange session identifiers for tracking a recording session between peers.

The Session-ID comprises of the following two Universally Unique Identifiers (UUIDs) corresponding to the initiator and recipient of the recording request respectively:

- Local UUID corresponds to UUID of the User Agent that sends a recording request to the participants of a recording session.
- Remote UUID corresponds to UUID of the User Agent that receives the recording request in a recording session.

Session-ID Handling

CUBE Media Proxy generates a unique UUID locally, and this UUID is passed as local UUID value in the Session-ID header of the following SIP request and response:

- Request to primary and optional recorders.
- Response to Unified CM (Network-Based Recording) or CUBE (SIPREC-Based).

The following events are involved in the Session-ID handling by CUBE Media Proxy:

1. The initial Invite received by CUBE Media Proxy includes a local UUID generated by the originating platform and a null remote UUID as shown in the following example.

```
Session-ID: db248b6cbdc547bbc6c6fd6b6916eeb;remote=00000000000000000000000000000000
```

2. When sending an Invite to the primary recorder, CUBE Media Proxy generates a new UUID to use for the local Session Identifier. The remote UUID remains null.

```
Session-ID: 8dfb2f2e1d4c518db6122080fb8b1d83;remote=00000000000000000000000000000000
```

3. The subsequent 200 OK response from the primary recorder includes a local session identifier that it generated and the UUID provided by CUBE Media Proxy in the Invite as the remote session identifier.

```
Session-ID: 4fd24d9121935531a7f8d750ad16e19;remote=8dfb2f2e1d4c518db6122080fb8b1d83
```

4. When sending a 200 OK to the originating platform, CUBE Media Proxy uses the UUID it generated as the local session identifier and the UUID it received initially as the remote session identifier.

```
Session-ID: 8dfb2f2e1d4c518db6122080fb8b1d83;remote=db248b6cbdc547bbc6c6fd6b6916eeb
```

5. CUBE Media Proxy sends a forking request to the remaining four recorders with Session-ID header containing the same locally generated UUID as the local UUID and a "NULL" value for the remote UUID.

```
Session-ID: 8dfb2f2e1d4c518db6122080fb8b1d83;remote=00000000000000000000000000000000
```

6. CUBE Media Proxy receives 200OK response from the remaining four recorders. The Session-ID header of the response message from each recorder contains UUID of the recorder as the local UUID and the locally generated UUID by the CUBE Media Proxy as the remote UUID.

```
Session-ID: 4fd24d9121935531a7f8d750ad17f20;remote=8dfb2f2e1d4c518db6122080fb8b1d83
```

7. In NBR mode, CUBE Media Proxy sends a SIP Info Message to Unified CM. For more information on SIP Info Message, see [SIP Info Messages from CUBE Media Proxy to Unified CM, on page 568](#). The Session-ID header of the SIP Info Message contains locally generated UUID by CUBE Media Proxy as local UUID and the UUID of Unified CM as the remote UUID.

```
Session-ID: 8dfb2f2e1d4c518db6122080fb8b1d83;remote=db248b6cbdc547bbc6c6dfb6916eeb
```

Recording State Notification

SIP Info Messages from CUBE Media Proxy to Unified CM

After trying or establishing an NBR session with the recorders, the CUBE Media Proxy sends SIP Info message to Unified CM to provide the consolidated status of all the recorders.

A SIP Info message is sent during the following stages of a recording session:

1. Initial Call: After receiving response from all the configured recorders during the initial call, a SIP Info message with status of each recorder is sent to the initiator of the recording session.
2. Mid-Call: When status of any of the recorders changes during the call, another SIP Info message with status of each recorder is sent to the initiator of the recording session. A change in status may result from any of the recorders sending a "BYE" or rejecting a midcall RE-INVITE.



Note The examples in the following sections illustrate CUBE Media Proxy forking to two of the maximum five destinations.

XML Format of a SIP Info Message

The Content-Type header present in the SIP Info message is:

```
Content-Type:application/x-cisco-proxy-recording-status+xml
```

The following is the XML format of a SIP info message.

```
<recorderList>
  <recorder>
    <uri>recorder1</uri>
    <recordertype>Mandatory</recordertype>
    <status>Success</status>
    <errormessage>null</errormessage>
  </recorder>
  <recorder>
    <uri>recorder2</uri>
    <recordertype>Mandatory</recordertype>
    <status>Failed</status>
    <errormessage>SIP error code received from Recorder</errormessage>
  </recorder>
</recorderList>
```

Table 77: Details of XML Tag and Data Type

XML Tag	Data Type
uri (Mandatory)	String
recordertype (Mandatory)	Enum (Mandatory, Optional)
status (Mandatory)	Enum (Success, Failed)
errormessage (Optional)	String



Note The primary recorder in a secure forking scenario functions the same way as a mandatory recorder functions in a nonsecure forking scenario except that the `recorderType` tag is shown as optional. The following is the XML format of a SIP INFO message in a combination of secure and nonsecure forking scenario:

```
<recorderList>
  <recorder>
    <recorderType>Optional</recorderType>
    <status>Success</status>
  </recorder>
  <recorder>
    <recorderType>Optional</recorderType>
    <status>Success</status>
  </recorder>
  <recorder>
    <recorderType>Optional</recorderType>
    <status>Success</status>
  </recorder>
  <recorder>
    <recorderType>Optional</recorderType>
    <status>Success</status>
  </recorder>
  <recorder>
    <recorderType>Optional</recorderType>
    <status>Success</status>
  </recorder>
</recorderList>
```

SIP Info Message Sent During the Initial Call

SIP Info Message Sent During the Initial Call (All the Recorders as Optional)

For information on how to configure the recorders as Optional, see Step 3 and Step 4 of [Configure Media Proxy, on page 574](#).

The SIP Info Message sent during a recording session depends on the scenarios that are given in the following table:

Table 78: Scenarios and Recorder Status During the Initial Call with All Recorders as Optional

Scenario	<status> of <i>recorder-1</i> in a SIP Info Message	<status> of <i>recorder-2</i> in a SIP Info Message
Call to the primary recorder <i>recorder-1</i> is established and forking to <i>recorder-2</i> is triggered successfully.	<success>	<success>
Call to the primary recorder <i>recorder-1</i> is established and forking to <i>recorder-2</i> is rejected with 503 Service Unavailable.	<success>	<failure>

Scenario	<status> of <i>recorder-1</i> in a SIP Info Message	<status> of <i>recorder-2</i> in a SIP Info Message
Call to the primary recorder <i>recorder-1</i> is established and there is no response from <i>recorder-2</i> to the forking request.	<success>	<failure>
Call to the recorder <i>recorder-1</i> and <i>recorder-2</i> is rejected with 503 Service Unavailable.	<failure>	<failure>
There is no response from <i>recorder-1</i> or <i>recorder-2</i> are down.	<failure>	<failure>
<i>recorder-1</i> and <i>recorder-2</i> responds to the call with a 488 Not Acceptable Here response.	<failure>	<failure>
<i>recorder-1</i> and <i>recorder-2</i> reponds to the call with a 600 Busy Everywhere response.	<failure>	<failure>

**Note**

- After a SIP Info Message is sent, a 200 OK response is received from the initiator of the recording session.
- In all failure scenarios, an error code is sent in the <errormessage>.

SIP Info Message Sent During the Initial Call (One Recorder as Mandatory and Remaining as Optional)

For information on how to configure the recorders as Mandatory, see Step 3, Step 4 and, Step 5 of [Configure Media Proxy](#), on page 574.

The SIP Info Message that is sent during a recording session depends on the scenarios that are given in the following table.

Table 79: Scenarios and Recorder Status During the Initial Call with a Mandatory Recorder

Scenario	<status> of <i>recorder-1</i> in a SIP Info Message	<status> of <i>recorder-2</i> in a SIP Info Message
Call to the mandatory recorder <i>recorder-1</i> is established and forking to the optional recorder <i>recorder-2</i> is triggered successfully.	<success>	<success>
Call to the mandatory recorder <i>recorder-1</i> is rejected with a failure message and hence the optional recorder <i>recorder-2</i> is not tried.	<failure>	<failure>

Scenario	<status> of <i>recorder-1</i> in a SIP Info Message	<status> of <i>recorder-2</i> in a SIP Info Message
Call to the mandatory recorder <i>recorder-1</i> is established and when the optional recorder <i>recorder-2</i> is tried, the mandatory recorder disconnects with a BYE.	<failure> Note BYE is sent in the <errormessage>.	<cancelled> Note The connection to the optional recorder is cancelled as the primary recorder disconnects.
After the call is established with a mandatory recorder <i>recorder-1</i> and the optional recorder <i>recorder-2</i> , the mandatory recorder disconnects with a BYE.	<failure> Note BYE is sent in the <errormessage>.	<disconnected> Note The optional recorder is disconnected.

**Note**

- After a SIP Info Message is sent, a 200 OK response is received from the initiator of the recording session. Unified CM sends a 415 Unsupported Media Type message if the INFO sent from CUBE Media Proxy has a malformed XML body.
- For all failure scenarios, an error code is sent in the <errormessage>.

Media Proxy Configuration

- [Configure Media Proxy for Network-Based Recording Solutions, on page 572](#)
- [Configure SIPREC Media Proxy, on page 577](#)

Configure Media Proxy for Network-Based Recording Solutions

Following are the steps to configure CUBE Media Proxy for Network-Based Recording:

1. [Configure Outbound Dial-Peers to the Recorders, on page 572.](#)
2. [Configure Media Proxy, on page 574.](#)
3. [Configure Inbound Dial-Peer from Unified CM, on page 576.](#)

Configure Outbound Dial-Peers to the Recorders

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *recorder-dial-peer-tag* voip**
4. **destination-pattern [+] *string***

5. `session protocol sipv2`
6. `session target ipv4:[recording-server-destination-address | recording-server-dns]`
7. `session transport [udp|tcp|tls]`
8. `voice-class sip srtp crypto <crypto-tag> OR srtp pass-thru`
9. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>dial-peer voice recorder-dial-peer-tag voip</code></p> <p>Example:</p> <pre>Device(config)# dial-peer voice 8000 voip</pre>	<p>Configures a recorder dial peer and enters dial peer voice configuration mode.</p>
Step 4	<p><code>destination-pattern [+] string</code></p> <p>Example:</p> <pre>Device(config-dial-peer)# destination-pattern 595959</pre>	<p>Specifies either the prefix or full E.164 number required to reach the recorder. A destination pattern must not include regular expressions in this case.</p> <p>Note Alternatively, "destination uri" may be used.</p>
Step 5	<p><code>session protocol sipv2</code></p> <p>Example:</p> <pre>Device(config-dial-peer)# session protocol sipv2</pre>	<p>Configures the VoIP dial peer to use Session Initiation Protocol (SIP).</p>
Step 6	<p><code>session target ipv4:[<i>recording-server-destination-address</i> <i>recording-server-dns</i>]</code></p> <p>Example:</p> <pre>Device(config-dial-peer)# session target ipv4:198.51.100.1</pre>	<p>Specifies the target network address for the recorder. Keyword and argument are as follows:</p> <ul style="list-style-type: none"> • ipv4: <i>destination address</i> --IP address of the media target. <p>Note Cisco Unified SIP Proxy may be used to route or load balance forked sessions between a group of recorders. In this case, the Unified SIP Proxy IPv4 address should be configured as the session target.</p>

	Command or Action	Purpose
Step 7	session transport [udp tcp tls] Example: Device(config-dial-peer)# session transport tcp	Configures a VoIP dial peer to use TCP. Using the session transport command, you can also configure UDP and TLS protocols.
Step 8	voice-class sip srtp crypto <crypto-tag> OR srtp pass-thru Example: Device(config-dial-peer)#voice-class sip srtp crypto 20 OR Device(config-dial-peer)#srtp pass-thru	Configures SRTP crypto profile on the dial-peer. OR Configure the SRTP pass through on the outbound dial-peer for incoming INVITE. Note <ul style="list-style-type: none"> • This step is optional and is required only for secure media forking. • The voice-class sip srtp crypto <crypto-tag> is configured for RTP-SRTP Interworking. • The srtp pass-thru is configured for SRTP-SRTP pass through.
Step 9	end Example: Device(config-dial-peer)# end	Returns to privileged EXEC mode.

Configure Media Proxy

Before you begin

For secure forking, outbound dial peers must be configured for TLS or SRTP. For further information, refer to [Configuring CUBE for SIP TLS](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile recorder** *profile-tag*
4. **media-recording proxy** [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]
5. **media-recording proxy secure** [*dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5*]
6. **proxy policy mandatory** *dial-peer-tag*
7. **exit**
8. **media class** *tag*
9. **recorder profile** *tag*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile recorder <i>profile-tag</i> Example: Device(config)# media profile recorder 100	Configures the media profile recorder and enters media profile configuration mode.
Step 4	media-recording proxy [<i>dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5</i>] Example: Device(cfg-mediaprofile)# media-recording proxy 8000 8001 8002	Configures the dial-peers for forking. The proxy configures the first dial-peer of the sequence for establishing a back-to-back (B2B) call, and the remaining dial-peers for media forking. Note You can specify maximum of five dial-peer tags.
Step 5	media-recording proxy secure [<i>dial-peer-tag1 dial-peer-tag2 dial-peer-tag3 dial-peer-tag4 dial-peer-tag5</i>] Example: Device(cfg-mediaprofile)# media-recording proxy secure 9000 9001 9002	From Cisco IOS XE Bengaluru 17.5.1a onwards, CUBE Media Proxy supports both secure and nonsecure forking. You can configure the dial-peers for both secure and nonsecure forking. The permitted number of configured secure and nonsecure dial peers for forking is five. The behaviour in Cisco IOS XE Bengaluru 17.4.1a and earlier releases is unchanged if there are no secure dial peers configured. Note <ul style="list-style-type: none"> • All secure dial peers must use the same voice class srtp-crypto profile.
Step 6	proxy policy mandatory <i>dial-peer-tag</i> Example: Device(cfg-mediaprofile)# proxy policy mandatory 8001	(Optional) Specifies the dial peer that must be connected before other forks are attempted.

	Command or Action	Purpose
		<p>Note</p> <ul style="list-style-type: none"> • The proxy policy mandatory command cannot be used when dial peers are configured using media recording proxy secure command. • Only one mandatory dial peer may be configured for each profile. • The mandatory dial peer must be one of those configured with the media-recording proxy command.
Step 7	<p>exit</p> <p>Example:</p> <pre>Device(cfg-mediaprofile)# exit</pre>	Exits media profile configuration mode.
Step 8	<p>media class tag</p> <p>Example:</p> <pre>Device(config)# media class 100</pre>	Configures a media class and enters media class configuration mode.
Step 9	<p>recorder profile tag</p> <p>Example:</p> <pre>Device(cfg-mediaclass)# recorder profile 100</pre>	Configures the media profile recorder.
Step 10	<p>exit</p> <p>Example:</p> <pre>Device(cfg-mediaclass)# exit</pre>	Exits media class configuration mode.

Configure Inbound Dial-Peer from Unified CM

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice call-manager-dial-peer-tag voip**
4. **incoming uri {from | request | to | via } tag**
5. **media-class tag**
6. (Optional) **srtp pass-thru**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>call-manager-dial-peer-tag</i> voip Example: Device(config)# dial-peer voice 1000 voip	Configures an inbound dial peer and enters dial peer voice configuration mode.
Step 4	incoming uri {from request to via } tag Example: Device(config-dial-peer)# incoming uri via 101	Configures the voice class that is used to match the VoIP dial-peer to the URI of an incoming call from Unified CM via the header in an incoming SIP Invite message. Note For more information on incoming uri command, see incoming uri .
Step 5	media-class tag Example: Device(config-dial-peer)# media-class 100	Configures media class on the inbound dial peer from Unified CM.
Step 6	(Optional) srtp pass-thru Example: Device(config-dial-peer)#srtp pass-thru	Configure the SRTP pass through on the inbound dial peer for incoming INVITE. Note This step is optional and is required only for secure media forking. The srtp pass-thru is configured for SRTP-SRTP pass through.
Step 7	exit Example: Device(cfg-mediaclass)# exit	Exits media class configuration mode.

Configure SIPREC Media Proxy

Following are the steps to configure SIPREC-based CUBE Media Proxy:

1. [Configure Outbound Dial-Peers to the Recorders, on page 572.](#)

2. [Configure Media Proxy, on page 574.](#)
3. Configure SIPREC on CUBE. For more information, see [Overview](#).

Verification of CUBE Media Proxy Configuration

You can verify the configuration of CUBE Media Proxy using Unified CM NBR and SIPREC-Based CUBE Media Proxy using the following **show** and **debug** commands.

- **debug voip fpi all** (for ASR devices only)
- **debug voip ccapi all**
- **debug voip recmsp all**
- **debug ccsip all**
- **debug ccsip messages**(for audio calls)

The CUBE Media Proxy sends INVITEs to the recorders with a single stream, which successfully forks the primary call to the recorders. INVITEs to recorders have a single m-line with a send-only attribute.

- **show voip rtp connections**

Displays Real-Time Transport Protocol (RTP) connections.

Example:

For CUBE Media Proxy with Unified CM NBR, recording sessions consist of two sets of RTP streams that are set up independently for near-end and far-end streams. The following example shows RTP connections from 198.51.100.1 is forked to three recorders 8.41.17.71 to 73.

This example shows NBR with 3 recorders. Two inbound INVITEs (one each for near-end or far-end).

```
Device# show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use:8
Port range not configured
Min   Max   Ports   Ports   Ports
Media-Address Range          Port  Port  Available  Reserved  In-use
Global Media Pool            8000  48198  19999      101        8
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP  RmtRTP    LocalIP    RemoteIP    MPSS
VRF
1  100      101      8218     8372     198.51.100.1  192.0.2.1    NO
NA
2  101      100      8220     9000     8.43.21.69   8.41.17.71   NO
NA
3  104      103      8222     9238     8.43.21.69   8.41.17.72   NO
NA
4  107      106      8224     9250     8.43.21.69   8.41.17.73   NO
NA
5  108      109      8226     8374     198.51.100.1  192.0.2.1    NO
NA
6  109      108      8228     9002     8.43.21.69   8.41.17.71   NO
NA
7  112      111      8230     9240     8.43.21.69   8.41.17.72   NO
NA
8  115      114      8232     9252     8.43.21.69   8.41.17.73   NO
```

```
NA
Found 8 active RTP connections
```

For CUBE Media Proxy using SIPREC, both near-end and far-end streams are established with the same inbound INVITE, which includes the detail in 2 m-lines. The following example shows how the inbound RTP connections are established before creating the RTP connections for five forks.

This example shows SIPREC with 5 recorders. One inbound INVITE (both near-end or far-end streams).

```
Device# show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 12
Port range not configured
Min  Max  Ports  Ports  Ports

Media-Address Range          Port  Port  Available  Reserved  In-use
Global Media Pool            8000  48198 19999      101       12

VoIP RTP active connections :
No.  CallId  dstCallId  LocalRTP  RmtRTP   LocalIP          RemoteIP          MPSS  VRF
-----
1    200     202        8108     6012    198.51.100.1    192.0.2.1        NO    NA
2    201     203        8110     6014    198.51.100.1    192.0.2.1        NO    NA
3    202     200        8112     6004    8.43.21.69      8.41.17.71       NO    NA
4    203     201        8114     8882    8.43.21.69      8.41.17.71       NO    NA
5    208     204        8116     6000    8.43.21.69      8.41.17.72       NO    NA
6    209     204        8118     8886    8.43.21.69      8.41.17.72       NO    NA
7    212     205        8120     6008    8.43.21.69      8.41.17.73       NO    NA
8    213     205        8122     9990    8.43.21.69      8.41.17.73       NO    NA
9    216     206        8124     6024    8.43.21.69      8.41.17.74       NO    NA
10   217     206        8126     9978    8.43.21.69      8.41.17.74       NO    NA
11   220     207        8128     6016    8.43.21.69      8.41.17.75       NO    NA
12   221     207        8130     9968    8.43.21.69      8.41.17.75       NO    NA

Found 12 active RTP connections
```

• show voip recmsp session

Displays active recording Media Service Provider (MSP) session information internal to CUBE Media Proxy.

Following is the sample output for CUBE Media Proxy using Unified CM NBR or SIPREC-Based CUBE Media Proxy:

```
Device# show voip recmsp session

REC MSP active sessions:
MSP Call-ID          AnchorLeg Call-ID          ForkedLeg Call-ID
-----
103                  99                          107
104                  99                          111
105                  99                          115
106                  99                          119

Found 4 active sessions
```

• show voip recmsp session detail call-id *call-id*

Displays detailed information about the recording MSP Call ID.

Example:

Following is the sample output for CUBE Media Proxy using Unified CM NBR:

```
Device# show voip recmsp session detail call-id 104
REC MSP active sessions:
Detailed Information
```

```

=====
Recording MSP Leg Details:
Call ID: 103
GUID : 7C5946D38ECD

AnchorLeg Details:
Call ID: 100
Forking Stream type: voice-nearend
Participant: 10000

Non-anchor Leg Details:
Call ID: 101
Forking Stream type: voice-farend
Participant: 708090

Forked Leg Details:
Call ID: 104
Voice Near End Stream CallID 104
Stream State ACTIVE
Found 1 active sessions

```

In SIPREC-based CUBE Media Proxy, there are two voice near-end streams for the forked call leg. Following is the sample output:

```

Device# show voip recmsp session detail call-id 208
RECMSMP active sessions:
Detailed Information
=====
Recording MSP Leg Details:
Call ID: 204
GUID : C710812A808A

AnchorLeg Details:
Call ID: 200
Forking Stream type: voice-nearend
Participant: sipp

Non-anchor Leg Details:
Call ID: 202
Forking Stream type: voice-farend
Participant: 9876

Forked Leg Details:
Call ID: 208
Voice Near End Stream CallID 208
Stream State ACTIVE
Voice Near End Stream CallID 209
Stream State ACTIVE
Found 1 active sessions

```

- **show voip rtp forking**

Displays RTP media-forking connections.

Example:

Following is the sample output for CUBE Media Proxy using Unified CM NBR:

```

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 8.41.17.72, remote port 9238, local port 8222
      codec g711ulaw, logical ssrc 0x53
      packets sent 29687, packets received 0
    stream type voice+dtmf-nearend (4): count 0
    stream type voice+dtmf-farend (6): count 0
    stream type video (7): count 0
    stream type video-nearend (8): count 0
    stream type video-farend (9): count 0
    stream type application (10): count 0
  Fork 2
    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 8.41.17.73, remote port 9250, local port 8224
        codec g711ulaw, logical ssrc 0x53
        packets sent 29687, packets received 0
      stream type voice+dtmf-nearend (4): count 0
      stream type voice+dtmf-farend (6): count 0
      stream type video (7): count 0
      stream type video-nearend (8): count 0
      stream type video-farend (9): count 0
      stream type application (10): count 0
    Fork 3
      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 8.41.17.72, remote port 9240, local port 8230
          codec g711ulaw, logical ssrc 0x58
          packets sent 2980, packets received 0
        stream type voice+dtmf-nearend (4): count 0
        stream type voice+dtmf-farend (6): count 0
        stream type video (7): count 0
        stream type video-nearend (8): count 0
        stream type video-farend (9): count 0
        stream type application (10): count 0
      Fork 4
        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 8.41.17.73, remote port 9252, local port 8232
            codec g711ulaw, logical ssrc 0x58
            packets sent 2980, packets received 0
          stream type voice+dtmf-nearend (4): count 0
          stream type voice+dtmf-farend (6): count 0
          stream type video (7): count 0
          stream type video-nearend (8): count 0
          stream type video-farend (9): count 0
          stream type application (10): count 0

```

Following is the sample output for SIPREC-Based CUBE Media Proxy:

```

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 2
      remote ip 8.41.17.72, remote port 6000, local port 8116
        codec g711ulaw, logical ssrc 0x53
        packets sent 29687, packets received 0

```

```

    remote ip 8.41.17.72, remote port 8886, local port 8118
    codec g711ulaw, logical ssrc 0x53
    packets sent 1296, packets received 0
    stream type voice+dtmf-nearend (4): count 0
    stream type voice+dtmf-farend (6): count 0
    stream type video (7): count 0
    stream type video-nearend (8): count 0
    stream type video-farend (9): count 0
    stream type application (10): count 0
Fork 2
    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 2
    remote ip 8.41.17.73, remote port 6008, local port 8120
    codec g711ulaw, logical ssrc 0x53
    packets sent 29687, packets received 0
    remote ip 8.41.17.73, remote port 9990, local port 8122
    codec g711ulaw, logical ssrc 0x53
    packets sent 1296, packets received 0
    stream type voice+dtmf-nearend (4): count 0
    stream type voice+dtmf-farend (6): count 0
    stream type video (7): count 0
    stream type video-nearend (8): count 0
    stream type video-farend (9): count 0
    stream type application (10): count 0
Fork 3
    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 2
    remote ip 8.41.17.74, remote port 6024, local port 8124
    codec g711ulaw, logical ssrc 0x53
    packets sent 29687, packets received 0
    remote ip 8.41.17.74, remote port 9978, local port 8126
    codec g711ulaw, logical ssrc 0x53
    packets sent 1296, packets received 0
    stream type voice+dtmf-nearend (4): count 0
    stream type voice+dtmf-farend (6): count 0
    stream type video (7): count 0
    stream type video-nearend (8): count 0
    stream type video-farend (9): count 0
    stream type application (10): count 0
Fork 4
    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 2
    remote ip 8.41.17.75, remote port 6016, local port 8128
    codec g711ulaw, logical ssrc 0x53
    packets sent 29687, packets received 0
    remote ip 8.41.17.75, remote port 9968, local port 8130
    codec g711ulaw, logical ssrc 0x53
    packets sent 1296, packets received 0
    stream type voice+dtmf-nearend (4): count 0
    stream type voice+dtmf-farend (6): count 0
    stream type video (7): count 0
    stream type video-nearend (8): count 0
    stream type video-farend (9): count 0
    stream type application (10): count 0

```

- **show call active voice compact**

Displays a compact version of voice CallsInProgress. An extra call leg is displayed for media forking.

Example:

Following is a sample using NBR:

```
Device# show call active voice compact
<callID> A/O/FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 8
 100   ANS      T644   g711ulaw  VOIP      P10000           192.0.2.1:8372
 101   ORG      T644   g711ulaw  VOIP      P708090          8.41.17.71:9000
 104   ORG      T643   g711ulaw  VOIP      P708090          8.41.17.72:9238
 107   ORG      T643   g711ulaw  VOIP      P708090          8.41.17.73:9250
 108   ANS      T642   g711ulaw  VOIP      P10000           192.0.2.1:8374
 109   ORG      T642   g711ulaw  VOIP      P708090          8.41.17.71:9002
 112   ORG      T641   g711ulaw  VOIP      P708090          8.41.17.72:5240
 115   ORG      T641   g711ulaw  VOIP      P708090          8.41.17.72:9252
```

Following is a sample output using SIPREC:

```
Device# show call active voice compact
<callID> A/O FAX T<sec> Codec      type      Peer Address      IP R<ip>:<udp>
Total call-legs: 6
 200 ANS      T644   g711ulaw  VOIP      P10000           192.0.2.1:8108
 202 ORG      T644   g711ulaw  VOIP      P708090          8.41.17.71:8112
 208 ORG      T643   g711ulaw  VOIP      P708090          8.41.17.72:8116
 212 ORG      T643   g711ulaw  VOIP      P708090          8.41.17.73:8120
 216 ORG      T643   g711ulaw  VOIP      P708090          8.41.17.74:8124
 220 ORG      T643   g711ulaw  VOIP      P708090          8.41.17.75:8128
```

- **show sip-ua calls**

Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls.

Example:

Following is the sample output for CUBE Media Proxy using Unified CM NBR:

```
Device# show sip-ua calls
Total SIP call legs:3, User Agent Client:2, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID      : 4091A49B-308911E8-8008EC4C-8D01D66C@192.0.2.1
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number    : 808808
Called Number     : 8453
Called URI        :
Bit Flags         : 0xC04018 0x80000100 0x80
CC Call ID        : 2
Local UUID        : c7351800dd135daba19758eac6b1dd70
Remote UUID       : ab9f4823802156aaaa8d62e04aaa2b96
Source IP Address (Sig) : 192.0.2.1
Destn SIP Req Addr:Port : [192.0.2.2]:9312
Destn SIP Resp Addr:Port : [192.0.2.2]:9312
Destination Name   :
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object    : 0x0
Media Mode         : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID     : 2
Stream Type        : voice-only (0)
```

```

Stream Media Addr Type : 1
Negotiated Codec      : g711ulaw (160 bytes)
Codec Payload Type    : 0
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID                : -1
Local QoS Strength    : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status      : None
Media Source IP Addr:Port: [192.0.2.1]:8002
Media Dest IP Addr:Port : [192.0.2.2]:9000
Mid-Call Re-Association Count: 0
SRTP-RTP Re-Association DSP Query Count: 0

```

```
Options-Ping    ENABLED:NO    ACTIVE:NO
```

Following is the sample output for SIPREC-based CUBE Media Proxy:

```

Device# show sip-ua calls
Total SIP call legs:6, User Agent Client:5, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID          : C711BA13-7E9B11EA-8090D6ED-255EEFA0@8.43.21.69
  State of the call   : STATE_ACTIVE (7)
  Substate of the call : SUBSTATE_NONE (0)
  Calling Number      : sipp
  Called Number       : 9876
  Called URI          : sip:9876@8.41.17.71:8881
  Bit Flags           : 0xC04018 0x90000100 0x80
  CC Call ID          : 101
  Local UUID          : eeabf35db3d25ca4b8276616cdcf5d15
  Remote UUID         : 8afa5ed7b8a052e29235bade4affcf9e
  Source IP Address (Sig) : 8.43.21.69
  Destn SIP Req Addr:Port : [8.41.17.71]:8881
  Destn SIP Resp Addr:Port: [8.41.17.71]:8881
  Destination Name     : 8.41.17.71
Number of Media Streams : 2
Number of Active Streams: 2
  RTP Fork Object      : 0x0
  Media Mode           : flow-through
Media Stream 1
  State of the stream   : STREAM_ACTIVE
  Stream Call ID        : 101
  Stream Type           : voice+dtmf (1)
  Stream Media Addr Type : 1
  Negotiated Codec      : g711ulaw (160 bytes)
  Codec Payload Type    : 0
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  QoS ID                : -1
  Local QoS Strength    : BestEffort
  Negotiated QoS Strength : BestEffort
  Negotiated QoS Direction : None
  Local QoS Status      : None
  Media Source IP Addr:Port: [8.43.21.69]:8112
  Media Dest IP Addr:Port : [8.41.17.71]:6005
Media Stream 2
  State of the stream   : STREAM_ACTIVE
  Stream Call ID        : 102
  Stream Type           : voice+dtmf (1)
  Stream Media Addr Type : 1
  Negotiated Codec      : g711ulaw (160 bytes)
  Codec Payload Type    : 0

```

```

Negotiated Dtmf-relay      : rtp-nte
Dtmf-relay Payload Type   : 101
QoS ID                    : -1
Local QoS Strength        : BestEffort
Negotiated QoS Strength   : BestEffort
Negotiated QoS Direction  : None
Local QoS Status          : None
Media Source IP Addr:Port : [8.43.21.69]:8114
Media Dest IP Addr:Port   : [8.41.17.71]:8883
Mid-Call Re-Association Count: 0
SRTP-RTP Re-Association DSP Query Count: 0

```

```
Options-Ping      ENABLED:NO      ACTIVE:NO
```

• show voip fpi calls

Displays the call (both inbound and outbound leg) information at the application level.

Example:

Following is the sample output for CUBE Media Proxy using Unified CM NBR:

```

Device#show voip fpi calls
Number of Calls : 1
-----
 confID      correlator  AcallID    BcallID    state      event
-----
 1005         1           1019       1020       ALLOCATED  DETAIL_STAT_RSP

```

As there are 2-m lines in the incoming invite to SIPREC-based CUBE Media Proxy, two FPI sessions are created. Following is the sample output:

```

Device#show voip fpi calls
Number of Calls : 2
-----
 confID      correlator  AcallID    BcallID    state      event
-----
 42           13          102         100        ALLOCATED  DETAIL_STAT_RSP
 41           14          99          101        ALLOCATED  DETAIL_STAT_RSP

```

• show media-proxy sessions

Displays the inbound and forked Call-ID, Session-ID, and dial peer tag details of the active recording sessions. The "Secure" field in the command output is tagged Y if the recording session is secure and N if the recording session is nonsecure. The "SIPREC" field in the command output is tagged Y for SIPREC-based recording session and N for Unified CM-based recording session.

Example:

```

Device# show media-proxy sessions
-----
No.      Call-ID          Session-ID          Dialpeer    Secure
SIPREC   Inbound/Forked  LocalUuid;RemoteUuid  Tag         (Y/N)
(Y/N)
-----
1        36770/-         a234a20672ce596d969c59ee9767f127;  3          N
Y
                                     aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

```

• show media-proxy sessions summary

Displays the active recording session details such as the dial peer tag, IP address, port number, number of failed recording sessions, and total number of recording sessions.

Example:

NBR:

Device# show media-proxy sessions summary

No Sessions	Inbound/Forked	Dialpeer-Tag	IP:Port	Total/Failed
1	Forked	100	ipv4:8.41.17.71:5060	2/0
2	Forked	200	ipv4:8.41.17.72:5060	2/0
3	Forked	300	ipv4:8.41.17.73:5060	2/0
4	Inbound	5678		2/0

SIPREC:

Device# show media-proxy sessions summary

No Sessions	Inbound/Forked	Dialpeer-Tag	IP:Port	Total/Failed
1	Forked	100	ipv4:8.41.17.71:5060	1/0
2	Forked	200	ipv4:8.41.17.72:5060	1/0
3	Forked	300	ipv4:8.41.17.73:5060	1/0
4	Forked	400	ipv4:8.41.17.74:5060	1/0
5	Forked	500	ipv4:8.41.17.75:5060	1/0
6	Inbound	5678		1/0

• **show media-proxy sessions call-id *call-id***

Displays the details of the inbound leg and all the forked legs that are associated with the specified SIP leg call-ID. MSP call-ID is not a valid call-ID for this command. Specify the CCAPI call identifier of the SIP leg.

Example:

```
Device# show media-proxy sessions call-id 101
CC Call-ID: 100 Inbound-leg
Dur: 00:00:15 tx: 0/0 rx: 1484/296800 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 192.0.2.1:8372 Local-Addr: 192.0.2.1:8218 rtt:0ms pl:0/0ms
Dialpeer-Tag: 5678 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: ab9f4823802156aaaa8d62e04aaa2b96

CC Call-ID: 101 Forked-leg (Primary)
Dur: 00:00:15 tx: 1484/296800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:9000 Local-Addr: 8.43.21.69:8220 rtt:0ms pl:0/0ms
Dialpeer-Tag: 100 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ab9f4823802156aaaa8d62e04aaa2b96 RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 104 Forked-leg
Dur: 00:00:15 tx: 1480/296000 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.72:9238 Local-Addr: 8.43.21.69:8222 rtt:0ms pl:0/0ms
Dialpeer-Tag: 200 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: dcdf882f0876890b930f3427be7fa5f6

CC Call-ID: 107 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.73:9250 Local-Addr: 8.43.21.69:8224 rtt:0ms pl:0/0ms
Dialpeer-Tag: 300 Negotiated-Codec: g711ulaw
```

```
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: 8df0863a6434263f60e50124dae649e6
```

- **show media-proxy sessions session-id WORD**

Displays the details of the Media Proxy recording sessions that are associated with the specified session-ID. To display the details of a specific call-leg, specify the complete session ID string as, *local-uuid;remote=remote-uuid*. Tokens that are allowed for *WORD* are '*', [0-9], [a-f], and [A-F].

Example:

```
Device# show media-proxy sessions session-id 6bde661e9767590b930f3427ad6e94e9
CC Call-ID: 100 Inbound-leg
Dur: 00:00:15 tx: 0/0 rx: 1484/296800 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 192.0.2.1:8372 Local-Addr: 192.0.2.1:8218 rtt:0ms pl:0/0ms
Dialpeer-Tag: 5678 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: ab9f4823802156aaaa8d62e04aaa2b96

CC Call-ID: 101 Forked-leg (Primary)
Dur: 00:00:15 tx: 1484/296800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:9000 Local-Addr: 8.43.21.69:8220 rtt:0ms pl:0/0ms
Dialpeer-Tag: 100 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ab9f4823802156aaaa8d62e04aaa2b96 RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 104 Forked-leg
Dur: 00:00:15 tx: 1480/296000 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.72:9238 Local-Addr: 8.43.21.69:8222 rtt:0ms pl:0/0ms
Dialpeer-Tag: 200 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: dcd882f0876890b930f3427be7fa5f6

CC Call-ID: 107 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.73:9250 Local-Addr: 8.43.21.69:8224 rtt:0ms pl:0/0ms
Dialpeer-Tag: 300 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: 8df0863a6434263f60e50124dae649e6
```

- **show media-proxy sessions metadata-session-id x-session-id**

Displays the details of the Media Proxy recording sessions based on the x-session-id present in the "From" header of the INVITE from Cisco Unified Communications Manager.

Example:

```
Device# show media-proxy sessions metadata-session-id 696dd5d3f7755c6abdc438e93d01febf

CC Call-ID: 108 Inbound-leg
Dur: 00:00:46 tx: 0/0 rx: 3105/578880 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 192.0.2.1:8374 Local-Addr: 198.51.100.1:8226 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 1 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 528b282b804c5fd098eaba3696c00de2 RemoteUUID: 4fd8036613424366fe00521d46ea16e3

CC Call-ID: 108 Forked-leg (Primary)
Dur: 00:00:46 tx: 3105/578880 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:9002 Local-Addr: 8.43.21.69:8228 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 2 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 4fd8036613424366fe00521d46ea16e3 RemoteUUID: 528b282b804c5fd098eaba3696c00de2
```

```

CC Call-ID: 112 Forked-leg
Dur: 00:00:46 tx: 3100/577880 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.72:9240 Local-Addr: 8.43.21.69:8230 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 3 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 528b282b804c5fd098eaba3696c00de2 RemoteUUID: 74ad4a4da25e71f2ba0cdc58b8e22f04

```

```

CC Call-ID: 115 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.73:9252 Local-Addr: 8.43.21.69:8232 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 4 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 528b282b804c5fd098eaba3696c00de2 RemoteUUID: 96c06c6fc4809314dc2efe7ada030ed6

```

Supported Features

Mid-Call Message Handling

CUBE Media Proxy using Unified CM NBR or SIPREC support midcall signaling events that involve RE-INVITES from the initiator of the recording session (Unified CM or CUBE) to the recorders. CUBE Media Proxy handles the RE-INVITES that request a session refresh, change in SDP for media address, direction or codec, or change SRTP crypto suite/key.

For NBR solutions, CUBE Media Proxy sends status updates of a midcall event to Unified CM using SIP Info messages.

When CUBE Media Proxy establishes a new set of forked sessions, the first is referred to as the primary. Where a destination is configured as mandatory, the destination is always the primary. Where all destinations are optional, the first successfully created session is the primary.

Perform the following steps to handle midcall messages:

1. On receipt of a RE-INVITE, CUBE Media Proxy sends the RE-INVITE to the primary recorder.
2. If the primary destination responds to the RE-INVITE with a BYE, then:
 - If the primary is mandatory, the call and all forks are stopped by sending BYE to the destinations and originator.
 - If the primary is optional, the BYE is acknowledged, but not passed back to the originator. The primary session is maintained in a dormant state and further midcall updates are blocked for the remainder of the call.
3. For other responses, the message from the primary is sent to the originator (Unified CM or CUBE).
4. Where the RE-INVITE requests a change in SDP or SRTP and only if this is successfully acknowledged (200 OK) by the primary, the RE-INVITE is sent to the other destinations.
5. If any of the other destinations respond to the RE-INVITE with a failure, CUBE Media Proxy clears that fork by sending a BYE to that destination. The status of this failed session is provided to Unified CM in an INFO message in NBR configurations.

Secure Recording of Secure Calls and Nonsecure Calls

Secure Recording of Secure Calls

With CUBE Media Proxy using Unified CM NBR, it is possible to extend encrypted calls to forked destinations. In this scenario, call signaling is secured using TLS for each connection between CUBE Media Proxy and Unified CM and recorders. As SRTP passthrough is used for media flows, the cipher suite and encryption key negotiated between Unified CM and the primary destination is used for all forks.

Refer to [Configuring SIP TLS](#) to secure signaling on Unified CM and forked legs. SRTP configuration is only required for the Unified CM.

Secure Recording of Nonsecure Calls

From Cisco IOS XE Bengaluru 17.5.1a, CUBE Media Proxy used in NBR or SIPREC mode may be configured to secure specific forked sessions when the original call is not encrypted. In this case, the primary destination must be secured and is treated in the same way as a mandatory destination as described in the message handling section above. Refer to [SIP TLS and SRTP-RTP interworking](#)

Support for High Availability

CUBE Media Proxy may be run on a high availability pair of platforms to ensure that calls and media forks are maintained if hardware failure. Call and forked session state is continuously synchronized between the platforms, ensuring that the standby can seamlessly take over media forwarding and call control if necessary.

High availability is available for CUBE Media Proxy configured for Unified CM NBR or SIPREC using either box-to-box or inbox redundancy options.

The following conditions apply when using CUBE Media Proxy high availability:

- Both Active and Standby platforms must have a common hardware and software configuration.
- Calls are synchronized by establishing a checkpoint with the standby on completion of each INVITE, REINVITE, UPDATE, or BYE message transaction.
- Connections that are not successfully established at the point of switchover are not maintained (as there is no checkpoint for the incomplete message transaction).
- In Unified CM NBR mode, checkpoint information includes call metadata, SRTP context and common session ID for all forked sessions. Checkpoints are created after message flows between a recorder and Unified CM are complete. For example, when an optional recorder sends a BYE, the checkpoint is created after CUBE Media Proxy receives the 200 OK response from Unified CM for the INFO message it sends.
- In SIPREC mode, checkpoint information includes common session ID, but not metadata.

You can use the following **show** commands to monitor the recording sessions on the Active and the Standby instances of CUBE Media Proxy:

- **show call active voice compact**
- **show voip rtp connections**
- **show voip recmsp session**
- **show media-proxy sessions**
- **show media-proxy sessions summary**

- **show sip-ua calls**

Media Latch

By default, CUBE Media Proxy using Unified CM NBR uses source address validation to check if the IP address and port details that are received in the UDP header of the RTP or SRTP packets match with the details in the SDP sent by the SIP User Agent. Packets without matching IP address and port are dropped.

In a typical SCCP-based BiB recording using Unified CM NBR CUBE Media Proxy, Unified CM first sends an SDP with the IP address and a dummy port to the CUBE Media Proxy to get the capabilities of CUBE Media Proxy. Unified CM then sends this SDP to the SCCP phone. The CUBE Media Proxy does not know the BiB IP address and port details of the SCCP phone. In these call flows, the IP address and port details in the media packets that are sent from BiB of the SCCP phone to SCCP phone, are different from the IP address and port details in the packets that are sent from Unified CM to the CUBE Media Proxy.

Media Latching is enabled on Unified CM NBR CUBE Media Proxy by default so that the CUBE Media Proxy learns the remote IP address and port details from the UDP transport header of the first RTP or SRTP packet. Media latching is turned on for every call that flows through the CUBE Media Proxy, and works for initial and midcall scenarios. Media Latching is enabled on the inbound leg (Unified CM leg), such that the media packets are accepted even if they are sent from a source IP address and port that is different from the IP address that is advertised in the SDP.



CHAPTER 57

WebSocket-Based Media Forking for Cloud Speech Services

- [Overview, on page 591](#)
- [Prerequisites, on page 593](#)
- [Benefits, on page 594](#)
- [Restrictions, on page 594](#)
- [Licensing for WebSockets in CUBE, on page 595](#)
- [Feature Characteristics, on page 597](#)
- [Error Strings in WebSocket Forking, on page 602](#)
- [Configure WebSocket-Based Forking, on page 603](#)
- [Configure CA Signed Certificates for SIP TLS Support in WebSockets, on page 606](#)
- [Verify WebSocket-Based Forking, on page 608](#)

Overview

From Cisco IOS XE Bengaluru 17.6.1a, CUBE can use WebSockets to handle media forking in a Cisco Unified Contact Center Enterprise (UCCE) solution deployment with Cloud Speech Services.

In a typical deployment, Cisco Unified Customer Voice Portal (Cisco Unified CVP) handles a customer call initially before it's transferred to an agent if necessary. If Cloud Speech Services are required, Cisco Unified CVP instructs CUBE to fork media (audio) to the Speech Server using WebSockets. While the call is transferred to the selected agent.

Forking Based on SIP Re-INVITE

When the call is transferred using a SIP Re-INVITE, Cisco Unified CVP includes details of the forking request in a JSON encoded MIME attachment. CUBE sends status information about the forked stream back to Cisco Unified CVP using INFO messages. When the WebSocket connection is successful, the RTP media packets are forked to the Speech Server by CUBE.

Forking Based on SIP INFO Message

Cisco Unified CVP can also trigger a WebSocket-based forking request through the SIP INFO message. The details of the forking request are included in a JSON body similar to a forking request received in re-INVITE. CUBE supports the INFO message with content type **application/x-cisco-record+json** for WebSocket forking.

An INFO-based forking request is successful if the INFO message containing the forking request is received after a successful call setup.



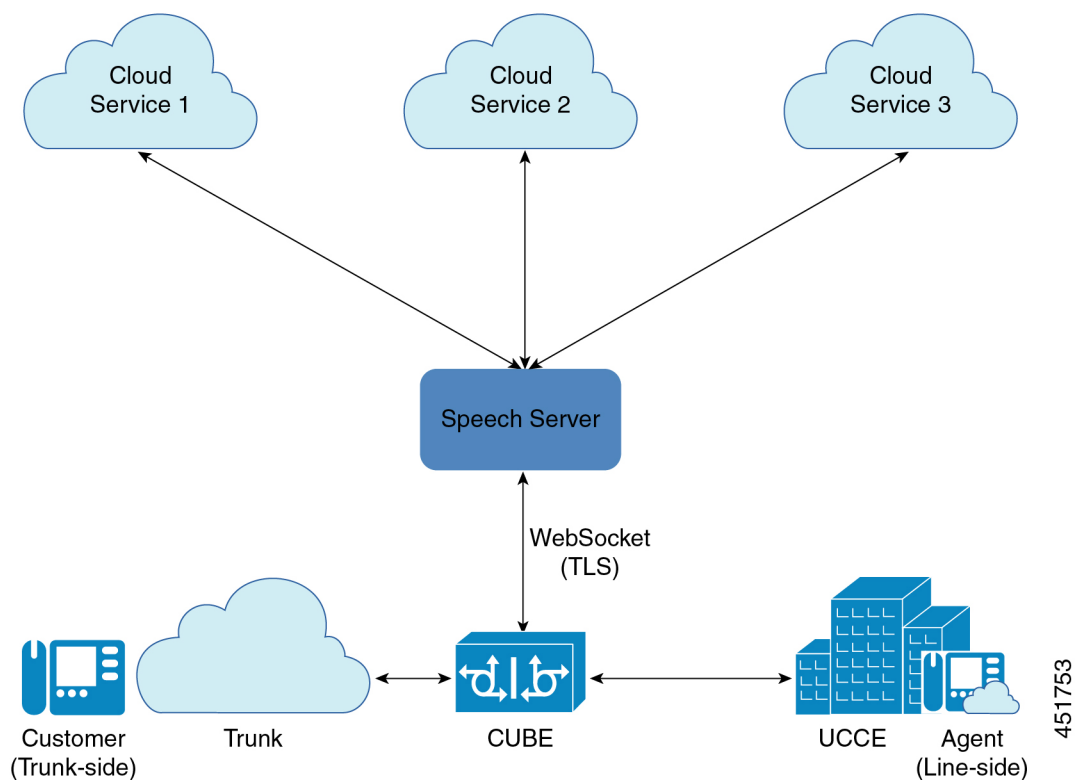
Note For more information on the supported and unsupported content types for SIP INFO message, see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_voi_unsupport_sipinfo_messages.html.

On receiving the forking request in the INFO message of the initial call, CUBE responds immediately to Cisco Unified CVP with a 200 OK message. Also, CUBE initiates a new WebSocket connection if there's no existing forking connection that can be reused for forking the incoming call. CUBE then identifies an existing WebSocket connection to transport the forked media. If there's no connection with available capacity, a new WebSocket connection is established. When a connection is identified, CUBE sends status information in an INFO message to CVP. Once the WebSocket connection is established, CUBE sends metadata to the speech server and starts forking the data packets.



Note If an INFO message is received outside of an existing call, CUBE rejects the request by responding with a 4XX message.

Figure 45: WebSockets in UCCE Solution Deployment





Note While WebSocket forking is enabled through configuration, CUBE only forks calls when explicitly requested with a SIP Re-INVITE or INFO message.

Feature Information

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 80: Feature Information

Feature Name	Releases	Feature Information
Secure WebSocket-based Media Forking on Cisco 4431, 4451-X, and 4461 Integrated Services Routers	Cisco IOS XE Bengaluru 17.6.2	WebSockets support media forking on Cisco 4431, 4451-X, and 4461 Integrated Services Routers.
WebSocket-based Media Forking for Cloud Speech Services	Cisco IOS XE Bengaluru 17.6.1a	WebSockets support media forking for Cloud Speech Services in CUBE.
GCM Ciphers for WebSocket-Based Media Forking	Cisco IOS XE Dublin 17.12.1a	This feature enables GCM cipher negotiation for TLS connectivity with the WebSocket server.

Prerequisites

Cisco IOS XE Bengaluru 17.6.1a or a later release that supports CUBE.

- WebSocket forking for CUBE is supported on the following platforms from Cisco IOS XE Bengaluru 17.6.1a:
 - Cisco Catalyst 8000V Edge Software (Catalyst 8000V)
- WebSocket forking for CUBE is supported on the following platforms from Cisco IOS XE Bengaluru 17.6.2:
 - Cisco 4431 Integrated Services Router
 - Cisco 4451-X Integrated Services Router

- Cisco 4461 Integrated Services Router

Benefits

WebSockets allow transportation of multiple media streams over a single reliable TLS connection, allowing more efficient use of network resources. As WebSockets use HTTPS ports, media streams can traverse firewalls without the need for special policies. Also, it's compatible with HTTP load balancers and proxies.

- CUBE supports a WebSocket deployment with HTTP 1.1 with the following characteristics:
 - Minimal state
 - Data format to stream multiple media sessions over a single connection.
 - No per-stream flow control and flow control is only at the TCP layer.

Restrictions

WebSocket-based forking doesn't support:

- Forking request in messages except Re-INVITE and INFO
- Doesn't support Websocket based forking on IPv6
- Both Re-INVITE and INFO message based forking in the same call. For example, CUBE cannot accept request to start forking (**START**) in Re-INVITE and stop forking (**STOP**) in the INFO message of the same call.
- Forking over Transport Layer Security (TLS) versions other than TLS 1.2
- Video forking
- Other forms of forking on the same CUBE instance
- Session Description Protocol (SDP) passthrough
- Codec payload buffering or VAD detection
- Secure Real-Time Transport Protocol (SRTP) passthrough calls.
- Forking isn't supported on an SRTP dial-peer.
- Call flows other than SIP to SIP.
- While WebSocket media forking can be used with CUBE High Availability architectures, if a switchover happens, active WebSocket media forks are cleared.
- ECDSA-based GCM ciphers isn't supported in the WebexCC Agent Answer infrastructure. Supports only RSA-based GCM ciphers.
- If the hostname gets resolved to multiple IP addresses, CUBE attempts connection on the first IP address only. That is, CUBE doesn't attempt connection with the remaining IP addresses if there's a connection failure with the first IP address.

Licensing for WebSockets in CUBE

A call that involves successful WebSocket forking in CUBE is counted as an Enhanced trunk call. If WebSocket forking is invoked midcall during a Standard trunk call, it is then considered as an Enhanced trunk call.



Note A call that involves WebSocket-based forking is considered successful if START message is sent to Speech Server and a WebSocket forking session is created.

The following licensing tags are used to track call counts in CUBE:

- CUBE Standard Trunk—License Tag to count the Standard trunk calls in CUBE.
- CUBE Enhanced Trunk—License Tag to count the Enhanced trunk calls in CUBE.
- CUBE Aggregate Trunk—Sum of Standard and Enhanced trunk calls in CUBE.

CUBE Modes and Licensing

- Box-to-Box High Availability (B2BHA) Mode—The CUBE Enhanced Trunk licensing tag is used to record all Enhanced trunk calls in CUBE for the B2BHA mode.
- Standalone Mode—The CUBE Enhanced Trunk and CUBE Standard Trunk licensing tags are used to record all standard and enhanced trunk calls in CUBE for the Standalone mode.
- Inbox High Availability Mode—The licensing for Inbox High Availability mode is similar to Standalone mode. The CUBE Enhanced Trunk and CUBE Standard Trunk licensing tags are used to record all Standard and Enhanced trunk calls in CUBE for the Inbox High Availability mode.

Following are some of the scenarios that are associated with licensing of CUBE calls that use WebSocket forking:

- A call with WebSocket forking is considered as an Enhanced trunk call until the call disconnects. The call is considered as Enhanced trunk call even if the WebSocket forking is stopped midcall.
- In a Call Transfer scenario, if the anchor leg is disconnected, the call involving WebSocket forking is no more treated as an Enhanced trunk call. It is considered as a Standard trunk call.
- A call is counted as an Enhanced trunk call only once even if:
 - WebSocket forking is invoked multiple times on a call leg.
 - WebSocket forking is invoked on both (incoming and outgoing) legs.
- Once a call is counted as an Enhanced trunk call, the call count is not altered even if there are further messages (Update, STOP, START) on the same leg.

High Availability Scenarios

- B2BHA calls in CUBE are counted as Enhanced trunk calls. Hence, when WebSocket forking is invoked on a B2BHA call, the Enhanced trunk call count is not incremented.

- All existing WebSocket forking sessions are cleared if there is a Stateful Switchover (SSO) in CUBE. However, new forking requests that are received after SSO are supported.
- As forking sessions are cleared during SSO, only the Standard trunk calls continue on the new active router.
- Information related to call counting gets checkpointed to the CUBE standby router.
- A B2BHA call continues as an Enhanced trunk call even if the WebSocket forking is stopped or even after SSO.
- High Availability calls in CUBE are checkpointed for serviceability and reporting (before and after SSO).
- Information about a call-leg using enhanced feature (that is, WebSockets) is checkpointed to the standby router from the active CUBE router. This information is used by the standby CUBE router to increment and decrement the call information correctly as Enhanced or Standard trunk call.



Note Inbox High Availability Mode and Standalone Mode use the same call counting logic.

License Usage

The count of calls in CUBE for a specific interval is required for license usage calculation. The following types of call counts are maintained in CUBE:

- CUBE Standard Trunk call count—Number of CUBE trunk calls that does not involve WebSocket forking.
- CUBE Enhanced Trunk call count—Number of CUBE calls involved in successful WebSocket forking.
- CUBE Aggregate Trunk call count—Sum of Enhanced and Standard trunk calls in CUBE.

License Usage Reporting

License usage reporting for the different CUBE modes are as follows:

- Box-to-Box High Availability (B2BHA) Mode—Peak usage value for the periodicity interval that is defined is reported by:
 - CUBE Enhanced Trunk tag for CUBE Enhanced calls (peak value).
- Standalone Mode—Peak usage value for the periodicity interval that is defined is reported by:
 - CUBE Enhanced Trunk tag.
 - CUBE Standard Trunk tag (Difference of peak value of CUBE Aggregate Trunk calls and CUBE Enhanced Trunk calls).
- Inbox High Availability Mode—Peak usage value for the periodicity interval that is defined is reported by:
 - CUBE Enhanced Trunk tag.

- CUBE Standard Trunk tag (Difference of peak value of CUBE Aggregate trunk calls and CUBE Enhanced trunk calls).



Note License reporting happens simultaneously for all CUBE tags. Separate timers are not maintained for any of the tags.

CUBE prints call history with data on the call count. The following is a sample call history with Enhanced and Aggregate trunk call count during call connect:

```
CUBE Standard Trunk call count: 0 , CUBE Enhanced Trunk Call count: 1, CUBE Aggregate Trunk
call count: 1 after WS_Fork_START
```

The following is a sample call history with Enhanced and Aggregate trunk call count during call disconnect:

```
CUBE Enhanced Trunk Call count: 0, CUBE Aggregate Trunk call count: 0 after call disconnected
```

Use the show command **show voice sip license stats table** to display the summary of last 10 license usage reports. For more information on license reporting periodicity and commands to verify the platform registration and license usage, see [Verify Smart License Operation, on page 35](#)

Feature Characteristics

- WebSockets fork SIP-to-SIP calls using G.711ulaw or G.711alaw.
- CUBE establishes a TCP connection with the destination URL provided in a forking request. The host address that is provided in the URL may either be an IPv4 address or a fully qualified domain name that is resolved using DNS. Once a connection is made with a destination, it can be used for multiple forked media streams. Two media streams are created for each forked call, one from the calling and one from the called party.
- CUBE uses INFO messages to provide connection status information to a Unified CVP and to signal the start of a stream to the Speech Server. Each stream is identified by a unique channel identifier.
- CUBE initiates a WebSocket connection by sending an HTTP GET request to the Speech Server with **Upgrade: websocket**. If the connection is successful, the speech server responds with **HTTP/1.1 101 Switching Protocols**. CUBE validates the connection by matching the Accept keys (**Sec-WebSocket-Accept**) that are exchanged in **GET** and **101** messages.
- The maximum number of WebSocket connections is based on the router platform.
- Established WebSockets maintain a persistent connection for as long as they are being used. A WebSocket connection is closed in either of the following ways:
 - If idle for more than 30 minutes, a WebSocket connection is closed automatically. To define a custom duration for the connection timeout, configure **connection idle-timeout minutes**.
 - Use the **clear voip stream-service connection id forced** command to clear a WebSocket connection.
- The following show commands display information about WebSockets in CUBE:
 - **show voip stream-service callid callid** —Displays detailed information about a WebSocket fork using the call ID of the original call.

- **show voip stream-service connection**—Displays information about all the active WebSocket connections in CUBE.
 - **show voip stream-service connection history**—Displays information about closed or stale WebSocket connections in CUBE.
 - **show voip stream-service connection id *id***—Displays detailed information about a specific WebSocket connection in CUBE.
 - **show voip stream-service server *ip:port***—Displays information about WebSocket connections corresponding to a specific Speech Server IP address and port.
 - **show voip stream-service statistics**—Displays statistical information about WebSocket connections in CUBE.
 - **show platform hardware qfp active feature sbc fork global**—Displays media forking statistics that are related to all the forking instances for an active Cisco Quantum Flow Processor (QFP) instance of CUBE.
 - **show platform hardware qfp active feature sbc fork session**—Displays media forking statistics specific to a fork session for an active Cisco Quantum Flow Processor (QFP) instance of CUBE.
- Use the **clear voip stream-service statistics** command to reset the global WebSocket statistics in CUBE.

Load Balancing

CUBE supports load balancing of forked media streams across multiple WebSocket connections. Each connection to a Speech Server can accommodate a maximum number of calls (threshold).

When CUBE receives a forking request, it assigns the media stream to one of the less busy connections to the target Speech Server. You can configure the maximum number of calls that CUBE assigns to each connection using the command **connection calls-threshold *calls***. The range is 1–20 calls. We recommend that you configure the default call threshold of three calls per connection.

Consider the following scenario. The threshold for the number of calls that a WebSocket connection can handle is ten. If all the WebSocket connections are handling ten calls each, then CUBE creates a new WebSocket connection for the incoming call.

Pause and Resume Forking

The codec that is used for a WebSocket fork must be the same as the one negotiated for the call. Consider a scenario in which CUBE receives an initial call with codec G711ulaw. If CUBE receives a forking request (re-INVITE with **START** message) with G711ulaw, then CUBE starts forking. However, if CUBE receives another re-INVITE with codec G711alaw during forking, a **PAUSE** message is sent to the Speech Server to suspend the forked stream.

CUBE sends a **PAUSE** message to the Speech Server to pause WebSocket-based forking in the following scenarios:

- A call with an ongoing forking session is placed on hold.
- A call with an ongoing forking session receives a re-INVITE with a codec other than the previously negotiated codec—In this scenario, codec information is available in the initial re-INVITE with the forking request.

WebSocket-based forking is resumed by sending a **RESUME** message to the Speech Server. The following are the prerequisites for CUBE to resume WebSocket-based forking:

- The forking is currently in the paused state.
- The call is currently not on hold.

The following are the scenarios in which CUBE resumes WebSocket-based forking.

- CUBE receives re-INVITE and the codec in the forking request is same as the negotiated codec.
- The call is placed on hold and the corresponding forking is paused. When the call is resumed, the forking is also resumed if:
 - The newly negotiated codec is same as the one received in the re-INVITE with a forking request.
 - The re-INVITE with a forking request doesn't have any codec information, and the call-negotiated codec is either G711ulaw or G711alaw.



Note WebSocket forking can only be used for g711ulaw and g711alaw codecs.

- CUBE sends a **PAUSE** message followed by a **RESUME** message even for a single re-INVITE forking request, in the following scenario. The initial re-INVITE with a forking request doesn't contain codec information. Call negotiation codec is either G711ulaw or G711alaw. Then CUBE uses either of these codecs (for example, G711alaw) to trigger forking. If CUBE receives a midcall re-INVITE with G711ulaw, it sends **PAUSE** followed by **RESUME** message. The **RESUME** message contains information on the newly negotiated codec.



Note • CUBE receives **START** and **STOP** in the re-INVITE or INFO message from Unified CVP to start and stop WebSocket-based forking respectively.

INFO-Based Forking

Some of the primary call scenarios and the corresponding behavior for INFO-based forking include:

- CUBE receives a Re-INVITE (with codec change, media address change or session refresh) request after the initial call is established—The Re-INVITE is handled as for a normal call. As INFO with JSON is received in the initial call, the CUBE triggers the forking request.
- CUBE receives a Re-INVITE after the initial call is established. INFO with JSON is received before completing the Re-INVITE transaction—As INFO with JSON is received in the initial call, CUBE triggers the forking request.
 - Re-INVITE for codec change introduces PAUSE and RESUME into the forking scenario.
 - Re-INVITE for media address change is handled consistent to the handling of a normal call.
 - Re-INVITE for session refresh is handled consistent to the handling of a normal call.

- CUBE successfully triggers a forking request but Unified CVP does not respond with 200 OK and retransmits INFO with JSON—CUBE ignores the retransmitted forking request.

UPDATE Message

Unified CVP can request CUBE to update the metadata in an ongoing forking session using the UPDATE message type. The metadata for the ongoing forking is in the JSON body of a Re-INVITE or INFO message.



Note The UPDATE message is contained in the JSON body of a SIP INFO message.



Note It's not allowed to use UPDATE message to change the forking session or connection. If a change in forking session or connection is required, use the STOP message to stop the current forking and the START message to restart forking with the new details.

Alarms

Alarms are generated corresponding to the events logged for WebSocket-based forking in CUBE. Alarms are generated in the form of syslog messages for the following events:

- Syslog Alarms
 - TCP failures—Failures while establishing a TCP connection. For example, an error while trying to set up a WebSocket connection with a server by providing the wrong IP address or port.
 - HTTP failures—Failures while establishing an HTTP connection, including authorization.
 - Remote WebSocket closure—An alarm is generated when the Speech Server closes a WebSocket connection gracefully.
 - TCP closure—An alarm is generated when a TCP connection to the Speech Server is closed unexpectedly.
- Alarms in Event Trace Logging

The following is a sample syslog alarm format specific to WebSocket-based forking:

```
%SIP-3-STREAM_SERVICE: 1 HTTP connection failures
%SIP-3-STREAM_SERVICE: 50 TCP connection failures
%SIP-3-STREAM_SERVICE: 60 Remote WebSocket closures
%SIP-3-STREAM_SERVICE: 120 TCP closures
```



Note By default, the syslog alarm is generated for the first instance of TCP failure, HTTP failure, Remote WebSocket closure, and TCP closure. Thereafter, CUBE generates syslog alarms for these events after every ten occurrences.

When you execute the command **clear voip stream-service statistics**, the statistics for the events TCP failure, HTTP failure, Remote WS closure and TCP closure are reset. The command **show voip stream-service statistics** displays these statistics.

Event Trace Logging

For WebSocket-based forking in CUBE, events are logged using the VoIP Trace and Event Trace Logging framework. While VoIP Trace logs the call events, Event Trace logs the global events and call events.

VoIP Trace logs call events that are related to WebSocket-based forking:

- Forking request for a call
- Forking initiated for a call
- Forking paused or resumed
- Forking stopped

Event Trace logs global events that are related to WebSocket-based forking:

- WebSocket creation
- WebSocket closure (Due to idle timeout)
- WebSocket closure (Due to clear command—**clear voip stream-service connection id**)
- WebSocket remote connection closure (Due to Speech Services closing the WebSocket connection gracefully)
- WebSocket TCP connection closure (Speech service outage is one of the identified causes)
- WebSocket connection creation failure
- Alarms. This is similar to Syslog Alarms.

The following is a sample output for Event Trace logging specific to WebSocket-based forking:

```
*Oct 14 07:18:10.913: CUBE_ET: TYPE = GLOBAL : WebSocket Connection creation successful for
ws://10.64.86.215:8000
*Oct 14 20:25:12.160: CUBE_ET: TYPE = GLOBAL : WebSocket Connection closed locally due to
idle-timeout expiry for ws://10.64.86.215:8000
*Oct 14 07:20:08.786: CUBE_ET: TYPE = GLOBAL : WebSocket Connection closed locally using
clear command for ws://10.64.86.215:8001
*Oct 14 21:01:38.061: CUBE_ET: TYPE = GLOBAL : WebSocket Connection was remotely closed for
ws://10.64.86.215:8002
*Oct 14 22:13:00.879: CUBE_ET: TYPE = GLOBAL : WebSocket Connection : 1 HTTP connection
failures
*Oct 14 07:18:31.205: CUBE_ET: TYPE = GLOBAL : WebSocket Connection was closed over TCP for
ws://10.64.86.215:8000
```

Server Name Indication (SNI)

WebSocket-based forking in CUBE provides support for Server Name Indication (SNI). SNI is a Transport Layer Security (TLS) extension that allows a TLS client to indicate the name of the server that it's trying to connect with during the initial TLS handshake process. The server hostname that is received in JSON by the WebSocket is used to configure SNI. SNI isn't set if the IP address of the host is received in JSON. For WebSocket-based forking, SNI is always used for WebSocket forking where possible.

If CUBE uses a proxy server for setting up a WebSocket connection, then SNI is set using the hostname of the proxy server that you configure. However, SNI isn't set if the IP address of the proxy server is configured instead of the hostname.

Common Name and Subject Alternate Name

WebSocket-based forking in CUBE supports server identity validation through Common Name and Subject Alternate Name fields in the server certificate. Common Name and Subject Alternate Name validation is supported only when the hostname of the server is available. Common Name and Subject Alternate Name isn't validated in WebSockets if CUBE receives the IP address of the host or proxy server.

For more information on SNI, Common Name and Subject Alternate Name, see [SIP TLS Support on CUBE](#).

Error Strings in WebSocket Forking

CUBE sends a SIP INFO message with the forking status to Cisco Unified CVP if an error occurs during an ongoing WebSocket forking.

Some of the forking related error strings originating from CUBE (toward Unified CVP) include:

Table 81: Error Strings in WebSockets

Error String	Error
Codec is not supported	Codec that is negotiated in the call or received in a forking request is not supported. WebSocket forking only supports G711ulaw and G711alaw codecs.
Connection failed	Unable to establish WebSocket connection with the Speech Server.
Internal error	Error occurred during the internal processing of WebSocket.
Connection closed	Closure of an idle WebSocket connection either locally or by the server. Closure of a WebSocket connection using a CLI command.
Authentication token invalid	Speech Server rejects the authentication token.
JSON parse failure	Parsing of the JSON content in the forking request failed.
Unexpected format or content in JSON	Unexpected value for a parameter in JSON. For example, " codec ": "g729" or " port ": "8080" (instead of " port ": 8080)
Mandatory parameter missing in JSON	One or more mandatory parameters are missing. For example, call-guid .
Method not supported	Request for an unsupported method received.
Invalid Start Fork Request	Out of sequence START message from CVP. For example, a forking session is active but CUBE receives START message.

Error String	Error
Invalid Stop Fork Request	CUBE receives out of sequence STOP message from Unified CVP. For example, fork session is inactive but CUBE receives STOP message.
DNS lookup failed	DNS lookup for the hostname (as received in JSON) of the Speech Server is unsuccessful.
Proxy DNS lookup failed	DNS Lookup for the proxy server that is configured is unsuccessful.
Unsupported flow	Active call flow uses an unsupported feature with WebSocket-based forking. For example, SRTP, FAX, SIPREC, SDP Passthrough, SIP-TDM, and so on. WebSocket forking is not enabled on the corresponding dial-peer.
Forking stopped	CUBE stops forking in response to the STOP request received from Unified CVP.
TCP Connection closed	TCP connection with the Speech Server is closed.
High availability Switchover	Switchover happens on CUBE and forking is stopped. Not applicable for CSR.
GUID Mismatch	GUID received in UPDATE message is different from START the message.
Invalid Update Fork Request	Out of sequence UPDATE message from CVP. For example, when a fork session is inactive, CUBE receives UPDATE message.

Configure WebSocket-Based Forking

Perform this task to configure WebSocket-based forking in CUBE.

Before you begin

- Cisco IOS XE Bengaluru 17.6.1a or a later release that supports CUBE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile stream-service tag**
4. (Optional) **secure-ciphersuite list**
5. (Optional) **connection { calls-threshold calls | idle-timeout minutes }**
6. **description string**
7. **proxy [host host port port | ip word port port string]**
8. **source-ip ip-address**

9. **exit**
10. **media class** *tag*
11. **stream-service profile** *tag*
12. **exit**
13. **dial-peer voice** *tag* **voip**
14. **media-class** *tag*
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enters privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	media profile stream-service <i>tag</i> Example: Device (config)# media profile stream-service 99	Enables stream-service on CUBE.
Step 4	(Optional) secure-ciphersuite <i>list</i> Example: Device (cfg-mediaprofile)# secure cipher-suite aes-128-cbc-sha	Configures the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(cfg-mediaprofile)# secure cipher-suite ecdhe-ecdsa-aes-gcm-sha2</pre>	<p>Note The following cipher suites are supported by WebSockets:</p> <ul style="list-style-type: none"> • aes-128-cbc-sha • dhe-rsa-aes-cbc-sha2 • ecdhe-rsa-aes-cbc-sha2 • rsa-aes-cbc-sha2 • ecdhe-ecdsa-aes-gcm-sha2 • ecdhe-rsa-aes-gcm-sha2 <p>WebSocket forking with GCM cipher suites includes AES256, and AES128 encryption algorithms:</p> <ul style="list-style-type: none"> • ecdhe-ecdsa-aes-gcm-sha2 includes ECDHE-ECDSA-AES256-GCM-SHA384 and ECDHE-ECDSA-AES128-GCM-SHA256. • ecdhe-rsa-aes-gcm-sha2 includes ECDHE-RSA-AES256-GCM-SHA384 and ECDHE-RSA-AES128-GCM-SHA256.
Step 5	<p>(Optional) connection { calls-threshold <i>calls</i> idle-timeout <i>minutes</i> }</p> <p>Example:</p> <pre>Device(cfg-mediaprofile)# connection idle-timeout 45</pre>	<p>Configures idle timeout and call threshold for a media profile in CUBE.</p> <ul style="list-style-type: none"> • If you don't provide any configuration, the default values are applied for timeout. Default for idle-timeout is 30 minutes. • The default for calls-threshold is three, and is the recommended call threshold value.
Step 6	<p>description <i>string</i></p> <p>Example:</p> <pre>Device(cfg-mediaprofile)# description <text></pre>	<p>Adds a description of up to 64 alphanumeric characters to a media profile.</p>
Step 7	<p>proxy [host <i>host</i> port <i>port</i> ip <i>word</i> port <i>port string</i>]</p> <p>Example:</p> <pre>Device(cfg-mediaprofile)# proxy ip 1.1.1.1 port 3456</pre>	<p>Configures the IP address or hostname of a WebSocket proxy server in CUBE.</p>
Step 8	<p>source-ip <i>ip-address</i></p> <p>Example:</p>	<p>Configures the local source IP address of a WebSocket connection in CUBE.</p>

	Command or Action	Purpose
	Device(cfg-mediaprofile)# source-ip 10.64.86.70	
Step 9	exit Example: Device(cfg-mediaprofile)# exit	Exits media profile configuration mode and enters global configuration mode.
Step 10	media class tag Example: Device(config)# media class 9	Configures a media class and enters media class configuration mode.
Step 11	stream-service profile tag Example: Device(cfg-mediaclass)# stream-service profile 99	Associates the details specific to stream-service with media class for WebSocket.
Step 12	exit Example: Device(cfg-mediaclass)# exit	Exits to global configuration mode.
Step 13	dial-peer voice tag voip Example: Device(config)# dial-peer voice 9090 voip	Defines a dial peer and enters the dial peer configuration mode.
Step 14	media-class tag Example: Device(config-dial-peer)# media-class 9	Binds the media class to a dial peer. It's mandatory to configure media-class and bind it to a dial peer to enable WebSocket forking. Otherwise, WebSocket-based forking is disabled for your dial-peer.
Step 15	end Example: Device(config-dial-peer)# end	Exits dial peer configuration mode and enters privileged EXEC mode.

Configure CA Signed Certificates for SIP TLS Support in WebSockets

For WebSocket forking to be supported over TLS, CUBE must perform CA certificate exchange with the remote server. To import the CA certificate and to configure the cipher suite that CUBE supports, perform the following steps:

Step 1 Configure trustpoint.**Example:**

The following is a sample configuration for RSA trustpoint:

```
configure terminal
crypto pki trustpoint websocket
    enrollment terminal
    revocation-check none
exit
```

Example:

The following are the steps to configure ECDSA trustpoint:

a. ECDSA key regeneration:

```
crypto key generate ec keysize 256 label ECK256
```

b. Configure ECDSA trustpoint:

```
configure terminal
crypto pki trustpoint ECDSA-DM
    enrollment terminal pem
    serial-number
    subject-name cn=MYSUB
    revocation-check none
    eckeypair ECK256
exit
```

c. CA certificate authentication:

```
crypto pki authenticate ECDSA-DM
```

For more information, see [Configuring Certificate Enrollment for a PKI](#).

Step 2 Import CA certificate for WebSockets.

Open Certificate in Notepad and copy-and-paste content from BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST.

Note Ensure that the clock on the CUBE router and the WebSocket server are consistent.

Example:

```
Router (config)#crypto pki authenticate websocket
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

Step 3 Bind the trustpoint with an HTTP client to be used for secure communication channels.**Example:**

```
configure terminal
http client secure-trustpoint websocket
```

Step 4 Configure the HTTP client to negotiate specified ciphers.

Note Starting from Cisco IOS XE Dublin 17.12.1a, GCM ciphers are also supported for WebSocket connections.

Example:

```
media profile stream-service tag
  secure-ciphersuite ecdhe-rsa-aes-gcm-sha2
```

Verify WebSocket-Based Forking

SUMMARY STEPS

1. **show run | sec media class**
2. **show run | sec dial-peer voice**
3. **show voip stream-service connection id *id***

DETAILED STEPS

Step 1 **show run | sec media class**

Show command output to verify **media class** configuration for WebSockets.

Example:

```
#show run | sec media class

media class 8
  stream-service profile 80
```

Step 2 **show run | sec dial-peer voice**

Show command to verify **media class** binding with a dial peer.

Example:

```
dial-peer voice 900 voip
  session protocol sipv2
  session target ipv4:8.41.17.71:7051
  session transport udp
  incoming called-number 6777
  dtmf-relay rtp-nte
  codec g711alaw

dial-peer voice 901 voip
  destination-pattern 6777
  session protocol sipv2
  session target ipv4:8.41.17.71:7052
  session transport udp
  media-class 8
  dtmf-relay rtp-nte
  codec g711alaw
```

Step 3 **show voip stream-service connection id *id***

The following is a sample output for the **show voip stream-service connection id** command displaying a GCM specific cipher secure WebSocket connection:

Example:

```
router# show voip stream-service connection id 60
Id: 60
Total session count: 1
Active session count: 1
Secure: Yes
TLS Version: TLS1.2
Cipher Suite: ECDHE-RSA-AES256_GCM-SHA384
Auth Token: e2238f3a-e43c-3f54-a05a-dd2e4bd4631f
Server Address: 10.1.40.50:8051
Local Address: 10.2.10.10:52642
State: Active
Connected at: Feb 7 07:47:27 UTC
```

```
Anchor leg cccallid          Data plane fork session id
      58                      2
```



PART IX

Security

- [SIP TLS Support, on page 613](#)
- [SRTP-SRTP Interworking, on page 633](#)
- [SRTP-RTP Internetworking, on page 649](#)
- [SRTP-SRTP Pass-Through, on page 663](#)
- [Monitoring of Phantom Packets, on page 669](#)
- [Security Compliance, on page 675](#)



CHAPTER 58

SIP TLS Support

- [Overview, on page 613](#)
- [Deployment, on page 614](#)
- [Restrictions, on page 617](#)
- [Prerequisites, on page 617](#)
- [Configure SIP TLS, on page 617](#)
- [Configure SIP TLS \(sip-ua\), on page 625](#)
- [Verify SIP TLS Configuration, on page 627](#)
- [Example: SIP TLS Configuration , on page 629](#)
- [Syslog Messages, on page 630](#)

Overview

The Cisco Unified Border Element (CUBE) supports secure SIP calls with Transport Layer Security (TLS). CUBE uses TLS over TCP transport to provide privacy and data integrity of SIP signaling messages it exchanges with remote services. TLS can be configured at the global, tenant and dial peer levels to secure signaling sessions with remote endpoints.

Feature Information

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.

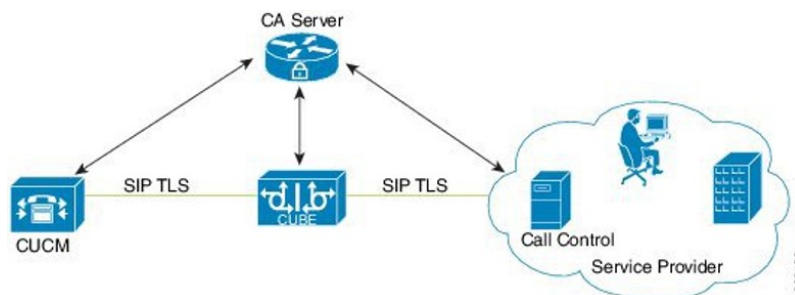
Table 82: Feature Information

Feature Name	Releases	Feature Information
Client Identity Validation through CN-SAN Fields in a TLS Certificate	Cisco IOS XE Cupertino 17.8.1a	Support introduced for CN-SAN validation of client certificate. The following commands under voice class tls-profile tag were updated or introduced: <ul style="list-style-type: none"> • cn-san validate { client bidirectional } • cn-san tag san-name
Configurable SIP Trunk Listen Port	Cisco IOS XE Cupertino 17.8.1a	Incoming calls may now be associated with a trunk by destination IP and port number.
Trunk Specific TLS Policy	Cisco IOS XE Cupertino 17.8.1a	Trunk specific TLS security trustpoint may now be defined in a tenant configuration. The voice class tls-cipher tag command was introduced to configure preferred TLS cipher options.
Secured SIP with TLS version 1.3 Support	Cisco IOS XE 17.14.1a	Transport Layer Security (TLS) version 1.3 support is introduced to enhance the security of CUBE flows. The supported TLS version 1.3 cipher suites are: <ul style="list-style-type: none"> • AES128_GCM_SHA256 • AES256_GCM_SHA384 • CHACHA20_POLY1305_SHA256 In addition, support for the minimum TLS version functionality with TLS version 1.2 is added. The following commands were modified: transport tcp tls , voice class tls-cipher , and show sip-ua connection tcp tls details .

Deployment

The following figure illustrates an example of CUBE with SIP TLS connections.

Figure 46: CUBE with SIP TLS connections



In a typical deployment, CUBE is placed between an enterprise calling solution such as CUCM, and the PSTN. These devices are authenticated and enrolled with a Certificate Authority (CA) server that issues certificates.

When making a call, a TLS session is created based on mutual trust established through PKI (public key infrastructure), which involves the exchange and validation of certificates signed by a trusted certificate authority (CA). This secure session is then used to send and receive SIP messages, including the sharing of symmetric keys used to encrypt media in associated SRTP streams.



Note PKI requires clients to use the correct time. It is recommended that all devices in a solution are synchronized with a common source using NTP.

TLS Versions

Starting from Cisco IOS XE 17.14.1a, TLS version 1.3 is supported in addition to TLS versions 1.0, 1.1 and 1.2. It is recommended that TLS version 1.2 or 1.3 is used wherever possible to ensure security or compliance.

- The TLS exclusivity functionality allows you to configure a particular version of TLS (1.0 or 1.1 or 1.2 or 1.3). It ensures that only the specified version is enabled for secure communication.
- The default behavior of the CLI command is enabled when none of the versions are specified. In the default form, all the TLS versions 1.1, 1.2, and 1.3 are supported. However, to configure TLS version 1.0, you must explicitly specify the TLS version.
- The minimum TLS version functionality is available only with TLS version 1.2. This minimum configuration enables TLS versions 1.2, and 1.3.

For the list of supported TLS cipher suites, see [TLS Cipher Suites](#).

Peer Verification

When establishing a TLS connection, there are several options for verifying the peer.

Certificate Verification

Every TLS session is verified by authenticating the certificate provided by the peer during the TLS exchange. Certificates may be self-signed, or signed by a mutually trusted Certificate Authority (CA). Provided that the certificate is found to be valid, the TLS session is established.

The limitation to this approach alone, is that it does not provide any assurance that the session is being established with the intended peer. For example, you may wish to connect with abc.com. In this case, CUBE would resolve the peer's fully qualified domain name using DNS and establish a connection with the resulting IP address. If this DNS resolution were compromised and the session established with a server at xyz.com with its own valid certificate, the session would still be established. To counter this possibility, the certified hostname of the peer should also be verified.

Hostname Verification

To ensure that a TLS session is established with the intended peer, CUBE can be configured to validate that hostname information provided in the peer's certificate is as expected. Both the Common Name (CN) and Subject Alternative Name (SAN) certificate fields are used to validate the peer.

Prior to Cisco IOS XE Cupertino 17.8.1a, CUBE was able to verify peer identity for outbound connections only, using the **cn-san-validate server** option. Here, the TLS session is established only if the Fully Qualified

Domain Name (FQDN) of the intended destination can be matched with the CN or SAN fields provided in the peer's certificate.

From Cisco IOS XE Cupertino 17.8.1a, CUBE can also verify peer identity for inbound connections. In this case the client provided certificate CN or SAN fields are matched against a list of preconfigured, permitted FQDNs. The **cn-san validate** command has been extended to include **client** and **bidirectional** options to configure inbound and/or outbound verification. The **cn-san** command is also used to configure a permitted list of FQDNs.

When an inbound TLS session is established using CN-SAN verification, the trusted IP address check is bypassed. You don't, therefore, need to add trust list IP addresses for peers that will be verified using CN-SAN.

Also from Cisco IOS XE Cupertino 17.8.1a, it is possible to configure CN-SAN verification and a list of trusted FQDNs in a TLS profile assigned to a tenant configuration. This allows you to craft unique TLS policies for each SIP trunk.

Remote Application Selection

To realise more efficient use of IP addresses, application service providers direct incoming TLS connections to different applications that share a common address using the TLS Server Name Indication (SNI) header. CUBE supports this concept, allowing the target application to be defined in a TLS policy. By associating a TLS policy that includes target SNI details with a tenant, all calls placed through the trunk are directed efficiently to the destination application.

TLS Cipher Suites

Cisco IOS XE supports the following TLS cipher suites, which may be configured, in preference order using the **voice class tls cipher** command.

Ciphers	Descriptions
AES128_GCM_SHA256	Supported in TLS 1.3
AES256_GCM_SHA384	Supported in TLS 1.3
CHACHA20_POLY1305_SHA256	Supported in TLS 1.3
DHE_RSA_AES128_GCM_SHA256	Supported in TLS 1.2
DHE_RSA_AES256_GCM_SHA384	Supported in TLS 1.2
DHE_RSA_WITH_AES_128_CBC_SHA	Supported in TLS 1.2 and below versions
DHE_RSA_WITH_AES_256_CBC_SHA	Supported in TLS 1.2 and below versions
ECDHE_RSA_AES128_GCM_SHA256	Supported in TLS 1.2
ECDHE_RSA_AES256_GCM_SHA384	Supported in TLS 1.2
ECDHE_ECDSA_AES128_GCM_SHA256	Supported in TLS 1.2
ECDHE_ECDSA_AES256_GCM_SHA384	Supported in TLS 1.2
RSA_WITH_AES_128_CBC_SHA	Supported in TLS 1.2 and below versions

Ciphers	Descriptions
RSA_WITH_AES_256_CBC_SHA	Supported in TLS 1.2 and below versions

Restrictions

- ECDSA ciphers are not supported with TLS version 1.0.
- WebSocket based media forking is not supported with TLS version 1.3.

Prerequisites

- Cisco 4000 series Integrated Services Routers (ISR4300 and ISR4400) require a security license to use TLS for SIP applications.
- For higher call volumes, you may also require a High Security (HSEC) license for your router.

Configure SIP TLS

Step 1: Create a certificate for CUBE to use

SUMMARY STEPS

1. `enable`
2. `configure terminal`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

Step 1a: Create a private key

SUMMARY STEPS

1. **crypto key generate rsa**{general-keys | usage-keys} [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *device*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>crypto key generate rsa{general-keys usage-keys} [label <i>key-label</i>] [exportable] [modulus <i>modulus-size</i>] [storage <i>device</i>]</p> <p>Example:</p> <pre>Router(config)# crypto key generate rsa general-keys label kp1 exportable</pre>	<p>Note Note: Alternatively to create an elliptic curve key, use crypto key generate ec keysize{256 384 512} [label <i>key-label</i>] [exportable]</p> <p>Generates RSA key pairs. Arguments and keywords are as follows:</p> <ul style="list-style-type: none"> • general-keys—Specifies that the general-purpose key pair should be generated. • usage-keys—Specifies that two RSA special-usage key pairs should be generated (that is, one encryption pair and one signature pair) instead of one general-purpose key pair. • label key-label—(Optional) Name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used. • exportable—(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router. • modulus modulus-size—(Optional) IP size of the key modulus in a range from 512 to 4096. If you do not enter the modulus keyword and specify a size, you will be prompted. • storage device:—(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).

Step 1b: Create a trustpoint to hold the certificate

SUMMARY STEPS

1. **crypto pki trustpoint** *name*
2. **rsa**keypair *key-label* [*key-size* [*encryption-key-size*]]
3. **fqdn** *CUBE FQDN*
4. (Optional) **serial-number** [**none**]

5. (Optional) **ip-address** [*ip-address* |*interface-name* |**none**]
6. **subject-name** *x.500-name*
7. **subject-alt-name** *fqdn*
8. **enrollment** [**mode** *ra*] [**retry period** *minutes*] [**retry count** *number*] [**terminal** [**pem**]] **url** *url* [**pem**]
9. **revocation-check** *method1* [*method2* [*method3*]]
10. **crl**
11. **password** *string*
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto pki trustpoint <i>name</i> Example: <pre>Router(config)# crypto pki trustpoint CUBE-TrustPoint</pre>	Declares the trustpoint that your router should use. Argument is as follows: <ul style="list-style-type: none"> • <i>name</i>—Creates a name for the trustpoint that you created. • <i>cube1</i>—Represents the trustpoint name that the user specifies.
Step 2	rsa keypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]] Example: <pre>Router(config)# rsa</pre>	<p>Note Alternatively use eckeypair <i>key-label</i> , if you have created an elliptic curve key.</p> <p>Specifies which key pair to associate with the certificate. Arguments are as follows:</p> <ul style="list-style-type: none"> • <i>key-label</i>—Name of the key pair, which is generated during enrollment if it does not exist or if the auto-enroll regenerate command is configured. • <i>key-size</i>—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • <i>encryption-key-size</i>—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.
Step 3	fqdn <i>CUBE FQDN</i> Example: <pre>Router (ca-trustpoint)# fqdn cube.example.com</pre>	Specifies Fully Qualified Domain Name (FQDN).
Step 4	(Optional) serial-number [none] Example: <pre>Router(ca-trustpoint)# serial-number</pre>	Specifies whether the router serial number should be included in the certificate request. Keyword is as follows: <ul style="list-style-type: none"> • none—(Optional) Specifies that a serial number will not be included in the certificate request.

Step 1b: Create a trustpoint to hold the certificate

	Command or Action	Purpose
Step 5	<p>(Optional) ip-address [<i>ip-address</i> <i>interface-name</i> none]</p> <p>Example:</p> <pre>Router(ca-trustpoint)# ip-address 172.18.197.154 GigabitEthernet2</pre>	<p>Specifies a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request. Arguments and keyword are as follows:</p> <ul style="list-style-type: none"> ip-address—Specifies a dotted IP address that will be included as "unstructuredAddress" in the certificate request. interface—Specifies an interface, from which the router can get an IP address, that will be included as "unstructureAddress" in the certificate request. none—Specifies that an IP address is not to be included in the certificate request.
Step 6	<p>subject-name <i>x.500-name</i></p> <p>Example:</p> <pre>Router(ca-trustpoint)# subject-name CN=cube.example.com</pre>	<p>Specifies the subject name in the certificate request. Argument is as follows:</p> <ul style="list-style-type: none"> x.500-name—(Optional) Specifies the subject name that is used in the certificate request.
Step 7	<p>subject-alt-name <i>fqdn</i></p> <p>Example:</p> <pre>Router (ca-trustpoint)# subject-alt-name cube.example.com</pre>	<p>Specifies the subject-alternate-name of the FQDN.</p>
Step 8	<p>enrollment [mode <i>ra</i>] [retry period <i>minutes</i>] [retry count <i>number</i>] [terminal [pem]] url <i>url</i> [pem]</p> <p>Example:</p> <pre>Router (ca-trustpoint)# enrollment url terminal</pre>	<p>Specifies the enrollment parameters of a certificate authority (CA). Arguments and keywords are as follows:</p> <ul style="list-style-type: none"> mode—(Optional) Registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled. retry period minutes—(Optional) Specifies the period in which the router waits before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 through 60 minutes.) retry count number—(Optional) Specifies the number of times a router resends a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 through 100 retries.) url url—URL of the file system where your router should send certificate requests. For enrollment method options, see the enrollment url command. terminal—includes the Privacy Enhanced Mail (PEM) encapsulation boundaries.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • pem—(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.
Step 9	<p>revocation-check <i>method1</i>[<i>method2</i>[<i>method3</i>]]</p> <p>Example:</p> <pre>Router(ca-trustpoint)# revocation-check none</pre>	<p>This describes one specific behaviour - that is revocation-check none. The command more generally defines how the router should check to see if the certificate in the trustpoint has been revoked by the CA.</p> <ul style="list-style-type: none"> • <i>method1</i> [<i>method2</i> [<i>method3</i>]]—Method used by the router to check the revocation status of the certificate. <p>Available methods are as follows:</p> <ul style="list-style-type: none"> • crl—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • none—Certificate checking is not required. • ocsp—Certificate checking is performed by an Online Certificate Status Protocol (OCSP). <p>Note If the second and the third methods are specified, each method will be used only if the previous method returns an error, such as the server being down.</p>
Step 10	<p>crl</p> <p>Example:</p> <pre>Router(ca-trustpoint)# crl</pre>	
Step 11	<p>password <i>string</i></p> <p>Example:</p> <pre>Router(ca-trustpoint)# password password</pre>	<p>(Optional) Specifies the revocation password for the certificate. Argument is as follows:</p> <ul style="list-style-type: none"> • <i>string</i>—Name of the password
Step 12	<p>exit</p> <p>Example:</p> <pre>Router# exit</pre>	Exists the current mode.

Step 1c: Create a certificate signing request

SUMMARY STEPS

1. `crypto pki enroll trustpoint`

Step 1d: Authenticate the trustpoint using the signing CA's certificate

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto pki enroll <i>trustpoint</i> Example: Device(config)# crypto pki enroll CUBE-TrustPoint	The Certificate Signing Request is displayed on the terminal. This should be sent to the Certificate Authority to generate a signed certificate.

Step 1d: Authenticate the trustpoint using the signing CA's certificate

SUMMARY STEPS

1. **crypto pki authenticate** *trustpoint*

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto pki authenticate <i>trustpoint</i> Example: crypto pki authenticate CUBE-TrustPoint	Paste the CA certificate when prompted so that the signed certificate can be authenticated when entered.

Step 1e: Import signed certificate

SUMMARY STEPS

1. **crypto pki import** <trustpoint> certificate

DETAILED STEPS

	Command or Action	Purpose
Step 1	crypto pki import <trustpoint> certificate Example: Router(config)# crypto pki import CUBE-TrustPoint certificate	Imports the certificate given by the CA using the method configured for the trustpoint.

Step 2: Configure preferred TLS cipher options

SUMMARY STEPS

1. **voice class tls-cipher** *tag*
2. **cipher preference** *cipher-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	voice class tls-cipher tag Example: <pre>Router(config)# voice class tls-cipher 100</pre>	Creates a cipher list with the provided tag number.
Step 2	cipher preference cipher-name Example: <pre>Router(config-class)# cipher 1 AES128_GCM_SHA256</pre>	Add up to 13 ciphers in order of preference.

Step 3: Configure TLS preferences with a TLS profile

SUMMARY STEPS

1. **voice class tls-profile tag**
2. **cipher cipher-list-tag**
3. **cn-san-validate [server | client | bidirectional]**
4. **trustpoint trustpoint-name**
5. **sni send**

DETAILED STEPS

	Command or Action	Purpose
Step 1	voice class tls-profile tag Example: <pre>Router(config)# voice class tls-profile 100</pre>	Creates a TLS profile with the provided tag number.
Step 2	cipher cipher-list-tag Example: <pre>Router(config-class)# cipher 100</pre>	The trustpoint label refers to the CUBE's certificate that is generated with the Cisco IOS PKI commands as part of the enrollment process. cipher 100 command argument, avoids changes to the configuration if SIP should mandate newer ciphers. The SSL layer in Cisco IOS does not support TLS_RSA_WITH_3DES_EDE_CBC_SHA. Therefore, CUBE actively uses only the TLS_RSA_WITH_AES_128_CBC_SHA suite in strict mode.
Step 3	cn-san-validate [server client bidirectional] Example: <pre>Router(config-class)# cn-san validate bidirectional</pre>	cn-san-validate {server client bidirectional} —Enables server identity validation through Common Name (CN) and Subject Alternate Name (SAN) fields in the server certificate during client initiated SIP/TLS connections. CUBE will only permit a TLS connection to be established if the domain name configured in the SIP session target is

	Command or Action	Purpose
		included in either the CN or SAN field of the certificate received from the server, client or both. Once you configure cn-san-validate { server client both }, the specified domain name check is carried out for every new TLS session.
Step 4	trustpoint trustpoint-name Example: <pre>Router(config-class)# trustpoint CUBE-TrustPoint</pre>	<ul style="list-style-type: none"> • trustpoint <i>string</i>—Refers to the trustpoint for the enrolled certificate.
Step 5	sni send Example: <pre>Router(config-class)# sni send</pre>	The sni send command enables Server Name Indication (SNI), a TLS extension that allows a TLS client to indicate the name of the server that it is trying connect during the initial TLS handshake process. Only the fully qualified DNS hostname of the server is sent in the client hello. SNI does not support IPv4 and IPv6 addresses in the client hello extension. After receiving a "hello" with the server name from the TLS client, the server uses appropriate certificate in the subsequent TLS handshake process. SNI is supported from TLS 1.2.

Step 4: Configure trunk or Tenant for TLS

SUMMARY STEPS

1. **voice class tenant** *tag*
2. **tls-profile** *tag*
3. **session transport tcp tls**
4. **listen-port secure** *port-number*
5. **url** {*sip* | *sips* | *tel*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	voice class tenant <i>tag</i> Example: <pre>Device(config)# voice class tenant 100</pre>	Enables tenant configuration mode.
Step 2	tls-profile <i>tag</i> Example: <pre>Device(config-class)# tls-profile 100</pre>	Associates the voice class TLS profile with the tenant. Tag range is 1—10000.

	Command or Action	Purpose
Step 3	session transport tcp tls Example: <pre>Router(voice class)# session transport tcp tls</pre>	Enable the session transport tcp tls.
Step 4	listen-port secure <i>port-number</i> Example: <pre>Device(config-class)# listen-port secure 5062</pre>	Configures the TLS listen port secure <i>port-number</i> in voice class tenant.
Step 5	url {<i>sip</i> <i>sips</i> <i>tel</i>} Example: <pre>Router(config-class)# url sips</pre>	Configures URLs to either the SIP, SIPS, or TEL format for your VoIP SIP calls. Keywords are as follows: <ul style="list-style-type: none"> • sip—Generate URLs in SIP format for VoIP calls. • sips—Generate URLs in SIPS format for VoIP calls. • tel—Generate URLs in TEL format for VoIP calls. This SIP gateway is now configured to use TLS with endpoints sharing the same CA. <p>Note This SIP gateway is now configured to use TLS with endpoints sharing the same CA.</p>
Step 6	end Example: <pre>Router(config-class)# end</pre>	Ends the current mode.

Configure SIP TLS (sip-ua)

Before you begin

Starting from Cisco IOS XE 17.14.1a, TLS version 1.3 is supported along with the existing TLS versions 1.2, 1.1, and 1.0. In addition, the support for **minimum** keyword configuration with TLS version 1.2 is introduced.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **transport {tcp [tls [v1.0 | v1.1 | v1.2 [minimum] | v1.3]] | udp}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	sip-ua Example: <pre>Device(config-voi-serv)# sip-ua</pre>	Enters voice service SIP user-agent configuration mode.
Step 4	transport {tcp [tls [v1.0 v1.1 v1.2 [minimum] v1.3]] udp} Example: <pre>Device(config-sip-ua)# transport tcp tls</pre>	<p>Configures the specified TLS version. Enables SIP user agent in TLS over TCP mode. The default configuration supports all TLS versions with fallback.</p> <ul style="list-style-type: none"> • Default configuration: Configured without specifying any specific TLS version. The TLS versions 1.1, 1.2, and 1.3 are supported except version 1.0. <pre>Device(config-sip-ua)# transport tcp tls</pre> • Exclusive version: Only the configured TLS version is enabled. <pre>Device(config-sip-ua)# transport tcp tls v1.3</pre> • Minimum TLS version: Only the configured TLS version ciphers or above version ciphers are supported. Fallback to previous version is not allowed. Note Supports the minimum keyword configuration only with TLS version 1.2. <pre>Device(config-sip-ua)# transport tcp tls v1.2 minimum</pre>

Verify SIP TLS Configuration

After a call is made, the following commands may be used to verify details of the TLS connection.

- **show sip-ua connections tcp tls brief**
- **show sip-ua connections tcp tls detail**
- The brief command displays the associated tenant (trunk) and listen port only.

Example brief Output

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

----- SIP Transport Layer Listen Sockets -----
Conn-Id      Local-Address      Tenant
=====
0             [0.0.0.0]:5061:    0
3             8.43.21.8:8888:    200
4             8.43.21.8:6061:    400
5             10.64.100.145:5091:vrf 44

Router#
```



Note The RSA or ECDSA key types in the detailed output are displayed only with TLS version 1.3.

The following is a sample output for the **show sip-ua connections tcp tls detail** command that displays RSA key type along with TLS version 1.3 ciphers:

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

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

```

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

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

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

```

The following is a sample output for the **show sip-ua connections tcp tls detail** command that displays ECDSA key type along with TLS version 1.3 ciphers:

```

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

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

Remote-Agent:10.1.10.50, Connections-Count:2
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
  TLS-Version Cipher Curve Tenant
  =====
  5061 9 Established 0 10.1.20.155:37081
  TLSv1.3 ECDHE-RSA-AES256-GCM-SHA384:ECDSA P-521 0
  41635 8 Established 0 10.1.20.155:5061
  TLSv1.3 TLS_AES_256_GCM_SHA384:ECDSA P-256 0

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

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

```

```

=====
0          [0.0.0.0]:5061:          0
1          [::]:5061:              0
6          [10.1.20.155]:5061:     0
7          [2001:10:1:20::135]:5061: 0
=====

```

Alternatively, the debug ccsip messages command can be used to verify the “Via:” header for TLS is included. This output is a sample INVITE request of a call that uses SIP TLS and the “sips:” URI scheme:

```

INVITE sips:777@172.18.203.181 SIP/2.0
Via: SIP/2.0/TLS 172.18.201.173:5060;branch=z9hG4bK2C419
From: <sips:333@172.18.201.173>;tag=581BB98-1663
To: <sips:5555555@172.18.197.154>
Date: Wed, 28 Dec 2005 18:31:38 GMT
Call-ID: EB5B1948-770611DA-804F9736-BFA4AC35@172.18.201.173
Remote-Party-ID: "Bob" <sips:+14085559999@1.2.3.4>
Contact: <sips:123@host>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO
Max-Forwards: 70
Cseq: 104 INVITE
Expires: 60
Timestamp: 730947404
Content-Length: 298
Content-Type: application/sdp

v=0
o=CiscoSystemsSIP-GW-UserAgent 8437 1929 IN IP4 172.18.201.173
s=SIP Call
c=IN IP4 1.1.1.1
t=0 0
m=audio 18378 RTP/AVP 0 19
c=IN IP4 1.1.1.1
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20

```

clear sip-ua tcp tls connection

Clear command to close a SIP TLS connection.

```

Router#clear sip-ua tcp tls connection ?
  id      Connection ID for the connection that needs to be closed in the sip tcp/udp process

  target  Target address for the connection that needs to be closed in the transport layer

Router#clear sip-ua tcp tls connection id ?
  <1-16380> Value of the Connection ID that needs to be closed

```

Example: SIP TLS Configuration

The following example provides excerpts from a typical running configuration.

```

show running-config brief
ip domain name example.com
!
crypto pki trustpoint CUBE-TrustPoint
  enrollment terminal
  fqdn cube.example.com
  subject-name cn=cube.example.com
  subject-alt-name cube.example.com
  revocation-check crl

```

```

    rsakeypair cube kp1
    !
crypto pki certificate chain CUBE-TrustPoint
    certificate 07
    !
voice class tenant 100
    tls-profile 100
    listen-port secure 5080
    sip-server dns:sip.acme.co:5080
    srtp-crypto 100
    session transport tcp tls
    url sips
    bind control source-interface GigabitEthernet0/0/0
    bind media source-interface GigabitEthernet0/0/0
    !
voice class srtp-crypto 100
    crypto 1 AEAD_AES_256_GCM
    crypto 2 AES_CM_128_HMAC_SHA1_80
    !
voice class tls-cipher 100
    cipher 1 DHE_RSA_AES128_GCM_SHA256
    !
voice class tls-profile 100
    cipher 100
    cn-san validate bidirectional
    cn-san 1 sip.acme.co
    trustpoint CUBE-TrustPoint
    !
dial-peer voice 100 voip
    description Towards sip.acme.co
    destination-pattern 1000
    session protocol sipv2
    session target sip-server
    voice-class codec 1
    voice-class sip tenant 100
    dtmf-relay rtp-nte
    no vad
    !

```

Syslog Messages

- From Cisco IOS XE Cupertino 17.8.1a, when CUBE fails to validate the peer certificate identity check through CN-SAN validation, a syslog message is generated in the following format:

```
Sep 26 07:15:57.949: %SIP-2-TLS_HANDSHAKE_FAILED :Peer certificate identity
check failed - remote_addr=198.51.100.254, remote_port=36233,
local_addr=203.0.113.254, local_port=3000, vrf=, tenant=1
```

- When there is a failure to open listen-socket for the associated tenant, a syslog message is generated in the following format:

```
Sep 24 05:32:27.838: %SIP-2-LISTEN_SOCKET: Failed to open listen socket for
ip_addr=198.51.100.255, port=8888, vrf=, transport=TLS, tenant=200
```

- From Cisco IOS XE 17.14.1a, when TLS handshake fails due to certificate mismatch, a syslog message is generated in the following format:


```
Dec 15 08:59:17.625: %SIP-2-TLS_HANDSHAKE_FAILED: Reason: certificate verify failed, Connection ID: 17, local address : [2001:10:2:10::10]:24399 and remote address : [2001:10:1:10::50]:5061
```

- From Cisco IOS XE 17.14.1a, when TLS handshake fails due to cipher mismatch, a syslog message is generated in the following format:

```
Dec 13 14:56:42.556: %SIP-2-TLS_HANDSHAKE_FAILED: Reason: no shared cipher, Connection ID: 12, local address : 10.04.200.100:5061 and remote address : 10.04.200.101:2009
```

- From Cisco IOS XE 17.14.1a, when TLS handshake fails due to version mismatch, a syslog message is generated in the following format:

```
Dec 8 04:02:47.096: %SIP-2-TLS_HANDSHAKE_FAILED: TLS handshake failure, Reason: tlsv1 alert protocol version, Connection ID: 8, local address : 10.04.200.101:5331 and remote address : 10.04.200.102:5061
```




CHAPTER 59

SRTP-SRTP Interworking

- [Overview, on page 633](#)
- [Restrictions, on page 636](#)
- [Configure SRTP-SRTP Interworking, on page 636](#)

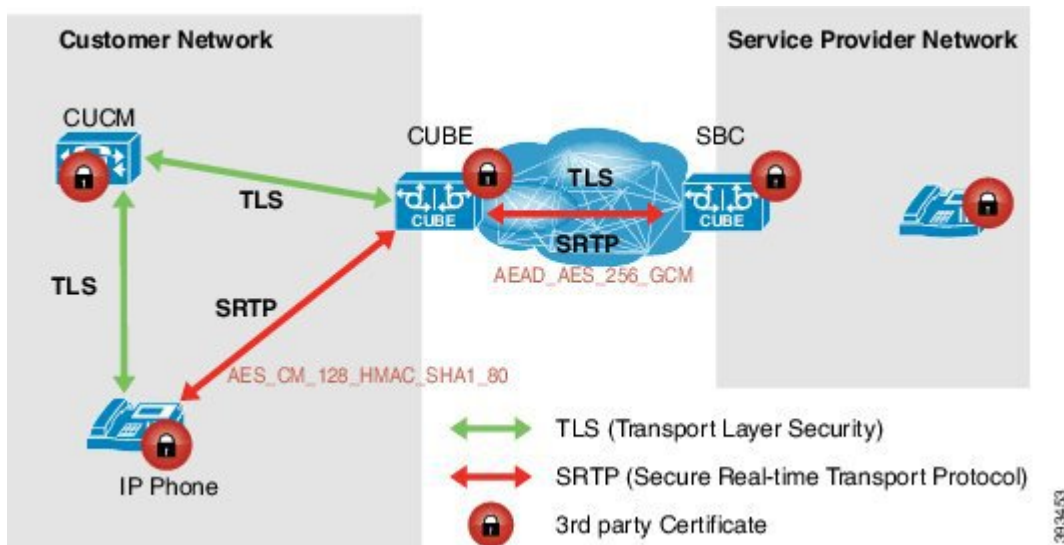
Overview

Cisco Unified Border Element (CUBE) supports secure calls between two networks having different cipher suites. SRTP-SRTP interworking is supported for audio and video calls.

From Cisco IOS XE Everest Release 16.5.1b onwards, when SRTP is enabled, by default Cisco Unified Border Element supports secure calls between networks using different cipher suites. The cipher suites supported for SRTP-SRTP interworking with default preference order is as follows:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Figure 47: SRTP-SRTP Interworking



CUBE allows you to change the list of preference order of the cipher-suites. Cipher-suite preference can be configured globally (under **voice service voip >> sip**), on a voice class tenant, or on a dial-peer.

The preference range is from 1 to 4, where 1 represents highest preference. CUBE offers SRTP cipher-suites in SDP offer based on the preference configured. For SDP answer, the highest configured preference cipher-suite that matches the offer from peer is selected.

Feature Information

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 83: Feature Information for SRTP-SRTP Interworking

Feature Name	Releases	Feature Information
Security Readiness Criteria (SRC)—Modified the command show sip-ua calls .	Cisco IOS XE Gibraltar Release 16.11.1a	Command show sip-ua calls is modified to display local crypto key and remote crypto key.

Feature Name	Releases	Feature Information
Support for SRTP-SRTP interworking	Cisco IOS XE Everest 16.5.1b	This feature allows secure calls between two enterprises using different cipher suites. Supported cipher suites are as follows: <ul style="list-style-type: none"> • AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_80 • AES_CM_128_HMAC_SHA1_32

Supplementary Services

The following supplementary services are supported:

- Midcall codec change with voice class codec configuration
- Reinvite-based call hold and resume.
- Music on hold (MoH) invoked from the Cisco Unified Communications Manager (Cisco UCM), where the call leg changes between SRTP and RTP for an MoH source.
- Reinvite-based call forward and call transfer.
- Call transfer based on a REFER message, with local consumption or pass-through of the REFER message on the CUBE
- Call forward based on a 302 message, with local consumption or pass-through of the 302 message on the CUBE
- T.38 fax switchover
- Fax pass-through switchover

For call transfers involving REFER and 302 messages (messages that are locally consumed on CUBE), end-to-end media renegotiation is initiated from CUBE only when you configure the **supplementary-service media-renegotiate** command in voice service VoIP configuration mode.



Note Any call-flow wherein there is a switchover from RTP to SRTP on the same SIP call-leg requires the **supplementary-service media-renegotiate** command that is enabled in global or voice service VoIP configuration mode to ensure that there is two-way audio.

Example call-flows:

- RTP-RTP flow switching to SRTP-RTP.
- Nonsecure MOH being played during secure call hold or resume.
- RTP-SRTP flow switching to SRTP- SRTP.

When supplementary services are invoked from the endpoints, the call can switch between SRTP and RTP during the call duration. Hence, Cisco recommends that you configure such SIP trunks for SRTP fallback. For information on configuring SRTP fallback, refer [Enable SRTP Fallback, on page 641](#).

Restrictions

- Asymmetric SRTP fallback configuration is not supported.
- Call Progress Analysis (CPA) is not supported.
- SRTP-SRTP calls with transcoding are only supported from Cisco IOS XE Bengaluru 17.6.1a onwards.
- SRTCP-RTCP interworking is not supported.
- More than one audio and video m-line is not supported.
- Unified CME and Unified SRST flows and SIP-TDM flows are not supported.
- GCM ciphers with extension header are not supported.

Configure SRTP-SRTP Interworking

Configure SRTP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *tag* voip**
4. **destination-pattern *string***
5. **session protocol sipv2**
6. **session target ipv4:*destination-address***
7. **incoming called-number *string***
8. **srtp**
9. **codec *codec***
10. **end**
11. **dial-peer voice *tag* voip**
12. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
13. **srtp**
14. **codec *codec***
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# dial-peer voice 201 voip	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> • In the example, the following parameters are set: <ul style="list-style-type: none"> • Dial peer 201 is defined. • VoIP is shown as the method of encapsulation.
Step 4	destination-pattern string Example: Device(config-dial-peer)# destination-pattern 5550111	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. <ul style="list-style-type: none"> • In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Specifies a session protocol for calls between local and remote routers using the packet network. <ul style="list-style-type: none"> • In the example, the sipv2 keyword is configured so that the dial peer uses the SIP protocol.
Step 6	session target ipv4:destination-address Example: Device(config-dial-peer)# session target ipv4:10.13.25.102	Designates an IP address where calls will be sent. <ul style="list-style-type: none"> • In the example, calls matching this outbound dial-peer will be sent to 10.13.25.102.
Step 7	incoming called-number string Example: Device(config-dial-peer)# incoming called-number 5550111	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. <ul style="list-style-type: none"> • In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	srtp Example: Device(config-dial-peer)# srtp	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 9	codec codec	Specifies the voice coder rate of speech for the dial peer.

	Command or Action	Purpose
	Example: Device(config-dial-peer)# codec g711ulaw	<ul style="list-style-type: none"> In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 10	end Example: Device(config-dial-peer)# end	Exits dial peer voice configuration mode.
Step 11	dial-peer voice tag voip Example: Device(config)# dial-peer voice 200 voip	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> In the example, the following parameters are set: <ul style="list-style-type: none"> Dial peer 200 is defined. VoIP is shown as the method of encapsulation.
Step 12	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 13	srtp Example: Device(config-dial-peer)# srtp	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 14	codec codec Example: Device(config-dial-peer)# codec g711ulaw	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 15	exit Example: Device(config-dial-peer)# exit	Exits dial peer voice configuration mode.

Configure Cipher Suite Preference (optional)



Note No additional configurations are required if you want to configure the default preference order. Use the following procedure for changing the default preference.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **voice class srtp-crypto tag**
4. **crypto preference cipher-suite**
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.
Step 3	voice class srtp-crypto tag Example: Device(config)# voice class srtp-crypto 100	Enters voice class configuration mode and assign an identification tag for a srtp-crypto voice class.
Step 4	crypto preference cipher-suite Example: Device(config-class)# crypto 1 AEAD_AES_256_GCM	Specifies the preference for an SRTP cipher-suite that will be offered by Cisco Unified Border Element (CUBE) in the SDP in offer and answer. You can configure a maximum of four preferences.
Step 5	exit Example: Device(config-class)# exit	Exists the present configuration mode.

What to do next

Assign SRTP Crypto voice class globally, or on a voice-class tenant, or on a dial-peer. For more information, see [Apply Crypto Suite Selection Preference \(optional\)](#), on page 639.

Apply Crypto Suite Selection Preference (optional)

Before you begin

- Ensure that an srtp voice-class is created using the **voice class srtp-crypto crypto-tag** command

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Apply crypto suite selection preference
 - In global configuration mode:

- **voice service voice**
 - **sip**
 - **srtp-crpto** *crypto-tag*
- In voice class tenant configuration mode:
 - **voice class tenant** *tag*
 - **srtp-crypto** *crypto-tag*
 - In dial-peer configuration mode:
 - **dial-peer voice** *tag voip*
 - **voice-class sip srtp-crypto** *crypto-tag*

4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Apply crypto suite selection preference <ul style="list-style-type: none"> • In global configuration mode: <ul style="list-style-type: none"> • voice service voice • sip • srtp-crpto <i>crypto-tag</i> • In voice class tenant configuration mode: <ul style="list-style-type: none"> • voice class tenant <i>tag</i> • srtp-crypto <i>crypto-tag</i> • In dial-peer configuration mode: <ul style="list-style-type: none"> • dial-peer voice <i>tag voip</i> • voice-class sip srtp-crypto <i>crypto-tag</i> Example:	Assigns previously configured crypto-suite selection preference. The <i>cryptp-tag</i> maps to the tag created using the voice class srtp-crypto command available in global configuration mode.

	Command or Action	Purpose
	<p>In global configuration mode:</p> <pre>Device> enable Device# configure terminal Device(config)# voice service voice Device(conf-voi-serv)# sip Device(conf-serv-sip)# srtp-crypto 102</pre> <p>In voice class tenant configuration mode:</p> <pre>Device> enable Device# configure terminal Device(config)# voice class tenant 100 Device(conf-serv-sip)# srtp-crypto 102</pre> <p>In dial-peer configuration mode:</p> <pre>Device> enable Device# configure terminal Device(config)# dial-peer voice 300 voip Device(config-dial-peer)# voice-class sip srtp-crypto 102</pre>	
Step 4	<p>end</p> <p>Example:</p> <pre>Device(config-dial-peer)# exit</pre>	Exits the present configuration mode.

Enable SRTP Fallback

You can configure SRTP with the fallback option so that a call can fall back to RTP if SRTP is not supported by the other call end. Enabling SRTP fallback is required for supporting nonsecure supplementary services such as MoH, call forward, and call transfer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - In dial-peer configuration mode

```
dial-peer
voice
tag
voip

srtp
fallback (for interworking with devices other than Cisco Unified Communications Manager)
```

or

voice-class sip srtp

negotiate cisco (Enable this CLI along with **srtp fallback** command to support SRTP fallback with Cisco Unified Communications Manager)

- In global VoIP SIP configuration mode

voice service voip**sip****srtp**

fallback(for interworking with devices other than Cisco Unified Communications Manager)

or

srtp

negotiate cisco (Enable this CLI along with **srtp fallback** command to support SRTP fallback with Cisco Unified Communications Manager)

4. exit**DETAILED STEPS**

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Enter one of the following commands: <ul style="list-style-type: none"> • In dial-peer configuration mode <p>dial-peer voice <i>tag</i> voip</p> <p>srtp fallback (for interworking with devices other than Cisco Unified Communications Manager)</p> <p>or</p> <p>voice-class sip srtp negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)</p> 	Enables call fallback to nonsecure mode.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • In global VoIP SIP configuration mode <pre> voice service voip sip srtp fallback(for interworking with devices other than Cisco Unified Communications Manager) or srtp negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager) Example: Device(config)# dial-peer voice 10 voip Device(config-dial-peer)# srtp fallback Example: Device(config)# dial-peer voice 10 voip Device(config-dial-peer)# voice-class sip srtp negotiate Cisco Example: Device(config)# voice service voip Device(config)# sip Device(conf-voi-serv)# srtp fallback Example: Device(config)# voice service voip Device(config)# sip Device(conf-voi-serv)# srtp negotiate cisco </pre>	
Step 4	<pre> exit Example: Device(conf-voi-serv)# exit </pre>	Exits present configuration mode and enters privileged EXEC mode.

Configuration Examples

Example: Configuring SRTP-SRTP Interworking

The following example shows how to configure support for SRTP-SRTP interworking. In this example, the incoming call leg preference is set to AEAD_AES_256_GCM crypto-suite and the outgoing call leg preference is set to AES_CM_128_HMAC_SHA1_80 crypto-suite.

Configure SRTP:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 300 voip
Device(config-dial-peer)# description "inbound dialpeer for 81560"
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# incoming called-number 81560
Device(config-dial-peer)# srtp
Device(config-dial-peer)# codec g711ulaw
Device(config-dial-peer)# end

Device(config)# dial-peer voice 400 voip
Device(config-dial-peer)# destination-pattern 81560
Device(config-dial-peer)# description "outbound dialpeer for 81560"
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.13.25.102
Device(config-dial-peer)# srtp
Device(config-dial-peer)# codec g711ulaw
```

Create a voice class srtp-crypto 100 and assign AEAD_AES_256_GCM crypto-suite with highest preference:

```
Device(config)# voice class srtp-crypto 100
Device(config-class)# crypto 1 AEAD_AES_256_GCM
```

Assign srtp-crypto 100 on incoming dial-peer:

```
Device(config)# dial-peer voice 300 voip
Device(config-dial-peer)# voice-class sip srtp-crypto 100
Device(config-dial-peer)# codec g711ulaw
Device(config-dial-peer)# srtp
```

Create a voice class srtp-crypto 103 and assign AES_CM_128_HMAC_SHA1_80 crypto-suite with highest preference:

```
Device> enable
Device# configure terminal
Device(config)# voice class srtp-crypto 103
Device(config-class)# crypto 1 AES_CM_128_HMAC_SHA1_80
```

Assign srtp-crypto 103 on outgoing dial-peer:

```
Device(config)# dial-peer voice 400 voip
Device(config-dial-peer)# voice-class sip srtp-crypto 103
Device(config-dial-peer)# codec g711ulaw
```

```
Device(config-dial-peer)# srtp
```

```
Device# show sip-ua calls
```

```
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
```

```
SIP UAC CALL INFO
```

```
Call 1
```

```
SIP Call ID           : 706E9625-C4FB11E6-8008AFC8-C0129831@10.25.15.63
  State of the call    : STATE_ACTIVE (7)
  Substate of the call : SUBSTATE_NONE (0)
  Calling Number       : 61230
  Called Number        : 81560
  Called URI           :
  Bit Flags            : 0xC04018 0x80000100 0x80
  CC Call ID           : 2
  Local UUID           : d5173c8551b25b06820edc687e50ab90
  Remote UUID          : 2e9094e33b815992a519f82abfae09d2
  Source IP Address (Sig) : 10.25.16.63
  Destn SIP Req Addr:Port : [10.13.25.102]:14560
  Destn SIP Resp Addr:Port: [10.13.25.102]:14560
  Destination Name     :
  Number of Media Streams : 1
  Number of Active Streams: 1
  RTP Fork Object       : 0x0
  Media Mode            : flow-through
Media Stream 1
  State of the stream   : STREAM_ACTIVE
  Stream Call ID        : 2
  Stream Type           : voice+dtmf (1)
  Stream Media Addr Type : 1
  Negotiated Codec      : g711ulaw (80 bytes)
  Codec Payload Type    : 0
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  QoS ID                 : -1
  Local QoS Strength     : BestEffort
  Negotiated QoS Strength : BestEffort
  Negotiated QoS Direction : None
  Local QoS Status       : None
  Media Source IP Addr:Port: [10.25.15.63]:8002
  Media Dest IP Addr:Port : [10.13.25.102]:14240
  Local Crypto Suite     : AES_CM_128_HMAC_SHA1_80
  Remote Crypto Suite    : AES_CM_128_HMAC_SHA1_80
  Local Crypto Key       : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
  Remote Crypto Key      : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
  Mid-Call Re-Association Count: 0
  SRTP-RTP Re-Association DSP Query Count: 0
```

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

```
SIP UAS CALL INFO
```

```
Call 1
```

```
SIP Call ID           : 1-8614@10.41.50.13
  State of the call    : STATE_ACTIVE (7)
  Substate of the call : SUBSTATE_NONE (0)
  Calling Number       : 61230
  Called Number        : 81560
  Called URI           : sip:81560@10.13.25.102:5060
  Bit Flags            : 0xC0401C 0x10000100 0x4
  CC Call ID           : 1
  Local UUID           : 2e9094e33b815992a519f82abfae09d2
  Remote UUID          : d5173c8551b25b06820edc687e50ab90
```

Example: Changing the Cipher-Suite Preference

```

Source IP Address (Sig ): 10.25.15.63
Destn SIP Req Addr:Port : [10.41.50.13]:14450
Destn SIP Resp Addr:Port : [10.41.50.13]:14450
Destination Name       : 10.41.50.13
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object       : 0x0
Media Mode            : flow-through
Media Stream 1
  State of the stream   : STREAM_ACTIVE
  Stream Call ID       : 1
  Stream Type          : voice+dtmf (0)
  Stream Media Addr Type : 1
  Negotiated Codec     : g711ulaw (80 bytes)
  Codec Payload Type   : 0
  Negotiated Dtmf-relay : rtp-nte
  Dtmf-relay Payload Type : 101
  QoS ID               : -1
  Local QoS Strength   : BestEffort
  Negotiated QoS Strength : BestEffort
  Negotiated QoS Direction : None
  Local QoS Status     : None
  Media Source IP Addr:Port: [10.25.15.63]:8000
  Media Dest IP Addr:Port  : [10.41.50.13]:14670
  Local Crypto Suite     : AEAD_AES_256_GCM
  Remote Crypto Suite    : AEAD_AES_256_GCM (
                          AEAD_AES_256_GCM
                          AEAD_AES_128_GCM )
  Local Crypto Key      : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z8765tVb2
  Remote Crypto Key     : bTQqZXbgFJddAlhE9wJGV3aKxo5vPV+Z2345tVb2
Mid-Call Re-Association Count: 0
SRTP-RTP Re-Association DSP Query Count: 0

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

```

Example: Changing the Cipher-Suite Preference

Specify SRTP cipher-suite preference:

```

Device> enable
Device# configure terminal
Device(config)# voice class srtp-crypto 100
Device(config-class)# crypto 1 AEAD_AES_256_GCM
Device(config-class)# crypto 2 AEAD_AES_128_GCM
Device(config-class)# crypto 4 AES_CM_128_HMAC_SHA1_32

```

The following is the snippet of **show running-config** command output showing the cipher-suite preference:

```

Device# show running-config
voice class srtp-crypto 100
crypto 1 AEAD_AES_256_GCM
crypto 2 AEAD_AES_128_GCM
crypto 4 AES_CM_128_HMAC_SHA1_32

```

If you want to change the preference 4 to `AES_CM_128_HMAC_SHA1_80`, execute the following command:

```

Device(config-class)# crypto 4 AES_CM_128_HMAC_SHA1_80

```


The following is the snippet of **show running-config** command output showing the change in cipher-suite:

```
Device# show running-config
voice class srtp-crypto 100
crypto 1 AEAD_AES_256_GCM
crypto 2 AEAD_AES_128_GCM
crypto 4 AES_CM_128_HMAC_SHA1_80
```

If you want to change the preference of AES_CM_128_HMAC_SHA1_80 to 3, execute the following commands:

```
Device(config-class)# no crypto 4
Device(config-class)# crypto 3 AES_CM_128_HMAC_SHA1_80
```

The following is the snippet of **show running-config** command output showing the cipher-suite preference overwritten:

```
Device# show running-config
voice class srtp-crypto 100
crypto 1 AEAD_AES_256_GCM
crypto 2 AEAD_AES_128_GCM
crypto 3 AES_CM_128_HMAC_SHA1_80
```




CHAPTER 60

SRTP-RTP Internetworking

- [Overview, on page 649](#)
- [Prerequisites, on page 653](#)
- [Restrictions, on page 653](#)
- [Configure SRTP-RTP Interworking, on page 653](#)
- [Configure Crypto Authentication, on page 656](#)
- [Enable SRTP Fallback, on page 658](#)
- [Verify SRTP-RTP, on page 661](#)

Overview

The Cisco Unified Border Element (CUBE) support for SRTP-RTP interworking feature allows secure network to non-secure network calls and provides operational enhancements for Session Initiation Protocol (SIP) trunks from Cisco Unified Call Manager and Cisco Unified Call Manager Express. Support for Secure Real-Time Transport Protocol (SRTP) to Real-Time Transport Protocol (RTP) interworking in a network is enabled for SIP-SIP audio calls.

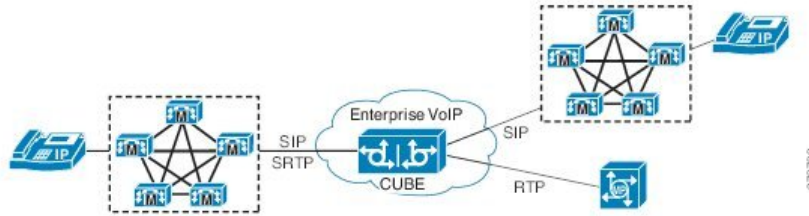
To configure support for SRTP-RTP interworking, you should understand the following concepts:

Support for SRTP-RTP Interworking

The CUBE support for SRTP-RTP Interworking feature connects SRTP Cisco Unified Call Manager domains with the following:

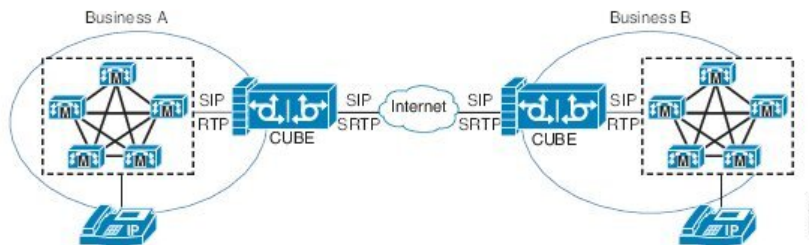
- RTP Cisco Unified Call Manager domains. Domains that do not support SRTP or is not configured for SRTP.
- RTP Cisco applications or servers. For example, Cisco Unified Meeting Place, Cisco WebEx, or Cisco Unity, which do not support SRTP, or is not configured for SRTP, or are resident in a secure data center.
- RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.

Figure 48: SRTP Domain Connections



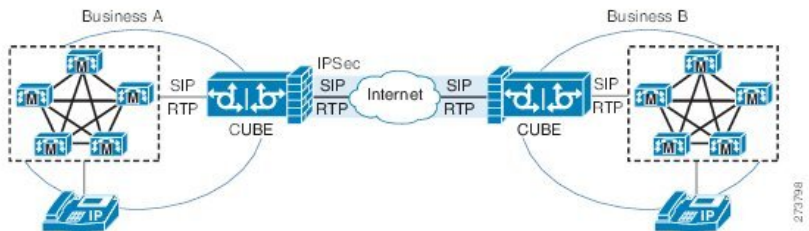
The CUBE support for SRTP-RTP interworking feature connects SRTP enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP interworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible and secure business-to-business communications without the need for static IPsec tunnels or the need to deploy SRTP within the enterprise.

Figure 49: Secure Business-to-Business Communications



SRTP-RTP interworking also connects SRTP enterprise networks with static IPsec over external networks.

Figure 50: SRTP Enterprise Network Connections



SRTP-RTP interworking on the CUBE in a network topology uses single-pair keygen. Existing audio and dual-tone multifrequency (DTMF) transcoding supports voice calls. There is no impact on SRTP-SRTP pass-through calls.

Use the **srtp** and **srtp fallback** commands to configure SRTP on one dial peer. Configure the RTP on the other dial peer. The dial peer configuration takes precedence over the global configuration on the CUBE.

Fallback handling occurs if one of the call endpoints does not support SRTP. The call can fall back to RTP-RTP, or the call can fail, depending on the configuration. Fallback takes place only if the **srtp fallback** command is configured on the respective dial peer.

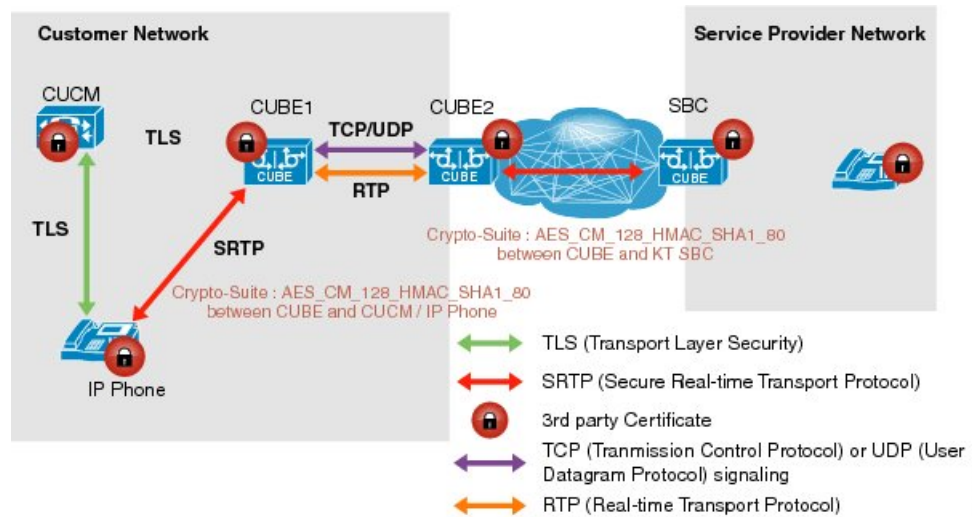
Use SRTP-RTP Chain for Interworking Between AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80 Crypto Suites

A single Cisco Unified Communications Manager (CUCM) device cannot terminate a Secure Real-Time Transport Protocol (SRTP) connection with an IP Phone using the AES_CM_128_HMAC_SHA1_32 crypto suite and initiate an SRTP connection with an external CUBE device with the AES_CM_128_HMAC_SHA1_80 crypto suite at the same time.

For Cisco Unified Communications Manager (Cisco Unified Communications Manager) and IP Phone devices that support only AES_CM_128_HMAC_SHA1_32 crypto suite, the interim SRTP-RTP interworking solution that is described below can be implemented.

- Cisco Unified Communications Manager or IP Phone side:
 - An SRTP connection using the AES_CM_128_HMAC_SHA1_32 crypto suite exists between the IP phone and CUBE1.
 - An RTP connection exists between CUBE1 and CUBE2.
- SIP trunk side—An SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite is initiated by CUBE2 here. In the image below, CUBE2 is the border element on the Customer Network and SBC is the border element on the Service Provider Network.

Figure 51: SRTP-RTP Interworking Supporting AES_CM_128_HMAC_SHA1_32 Crypto Suite



Note

- AES_CM_128_HMAC_SHA1_32 to AES_CM_128_HMAC_SHA1_80 interworking does not support to Cisco IOS XE Everest 16.4.1 Release.
- SRTP-SRTP interworking supports from Cisco IOS XE Everest 16.5.1b Release onwards, and therefore does not require an SRTP-RTP chain.

Supplementary Services Support

The following supplementary services are supported:

- Midcall codec change with voice class codec configuration
- Invite-based call hold and resume
- Music on hold (MoH) invoked from the Cisco Unified Communications Manager (Cisco UCM), where the call leg changes between SRTP and RTP for an MoH source
- Invite-based call forward and call transfer
- Call transfer based on a REFER message, with local consumption or pass-through of the REFER message on the CUBE
- Call forward based on a 302 message, with local consumption or pass-through of the 302 message on the CUBE
- T.38 fax switchover
- Fax pass-through switchover

For call transfers involving REFER and 302 messages (messages that are locally consumed on CUBE), end-to-end media renegotiation is initiated from CUBE only when you configure the **supplementary-service media-renegotiate** command in voice service voip configuration mode.



Note Any call-flow wherein there is a switchover from RTP to SRTP on the same SIP call-leg requires the **supplementary-service media-renegotiate** command enabled in global or voice service voip configuration mode to ensure there is 2-way audio.

Example call-flows:

- RTP -SRTP transfer on CUCM side
 - Non-secure MOH being played during secure call hold or resume
-

When supplementary services are invoked from the end points, the call can switch between SRTP and RTP during the call duration. Hence, Cisco recommends that you configure such SIP trunks for SRTP fallback. For information on configuring SRTP fallback, refer [Enable SRTP Fallback, on page 658](#) .

Feature Information

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 84: Feature Information for SRTP-RTP Interworking

Feature Name	Releases	Feature Information
Support for AEAD_AES_GCM_256 and AEAD_AES_GCM_128 crypto-suites	Cisco IOS XE Everest 16.5.1b	AEAD_AES_GCM_256 and AEAD_AES_GCM_128 crypto suites were added to support SRTP-RTP interworking.

Prerequisites

- SRTP-RTP interworking is supported with Cisco Unified Call Manager 7.0 and later releases.
- Platforms running on Cisco IOS XE Releases do not require DSP resources.

Restrictions

- More than one video m-line is not supported.
- GCM ciphers with extension header are not supported.

Configure SRTP-RTP Interworking



Note From Cisco IOS XE Everest Release 16.5.1b onwards, the following crypto suites are enabled by default on the SRTP leg:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Use the following procedure for changing the default preference list.

Perform the task in this section to enable SRTP-RTP interworking support between one or multiple Cisco Unified Border Elements for SIP-SIP audio calls. In this task, RTP is configured on the incoming call leg and SRTP is configured on the outgoing call leg.



Note This feature is available only on Cisco IOS XE images with security package.

SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **dial-peer voice tag voip**
4. **destination-pattern string**
5. **session protocol sipv2**
6. **session target ipv4: destination-address**
7. **incoming called-number string**
8. **codec codec**
9. **end**
10. **dial-peer voice tag voip**
11. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
12. **srtp**
13. **codec codec**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# dial-peer voice 201 voip	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> • In the example, the following parameters are set: <ul style="list-style-type: none"> • Dial peer 201 is defined. • VoIP is shown as the method of encapsulation.
Step 4	destination-pattern string Example: Device(config-dial-peer)# destination-pattern 5550111	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. <ul style="list-style-type: none"> • In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	session protocol sipv2 Example: Device(config-dial-peer)# session protocol sipv2	Specifies a session protocol for calls between local and remote routers using the packet network. <ul style="list-style-type: none"> • In the example, the sipv2 keyword is configured so that the dial peer uses the SIP protocol.

	Command or Action	Purpose
Step 6	session target <i>ipv4: destination-address</i> Example: Device(config-dial-peer)# session target ipv4:10.13.25.102.	Designates an IPv4 destination address where calls will be sent. <ul style="list-style-type: none"> In the example, calls matching this outbound dial-peer will be sent to 10.13.25.102.
Step 7	incoming called-number <i>string</i> Example: Device(config-dial-peer)# incoming called-number 5550111	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. <ul style="list-style-type: none"> In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	codec <i>codec</i> Example: Device(config-dial-peer)# codec g711ulaw	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 9	end Example: Device(config-dial-peer)# end	Exits dial peer voice configuration mode.
Step 10	dial-peer voice <i>tag voip</i> Example: Device(config)# dial-peer voice 200 voip	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> In the example, the following parameters are set: <ul style="list-style-type: none"> Dial peer 200 is defined. VoIP is shown as the method of encapsulation.
Step 11	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 12	srtp Example: Device(config-dial-peer)# srtp	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 13	codec <i>codec</i> Example: Device(config-dial-peer)# codec g711ulaw	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 14	exit Example: Device(config-dial-peer)# exit	Exits dial peer voice configuration mode.

Example: SRTP-RTP Interworking

The following example shows how to configure support for SRTP-RTP interworking. In this example, the incoming call leg is RTP and the outgoing call leg is SRTP.

```
%SYS-5-CONFIG_I: Configured from console by console
dial-peer voice 201 voip
 destination-pattern 5550111
 session protocol sipv2
 session target ipv4:10.13.25.102
 incoming called-number 5550112
 codec g711ulaw
!
dial-peer voice 200 voip
 destination-pattern 5550112
 session protocol sipv2
 session target ipv4:10.13.2.51
 incoming called-number 5550111
 srtp
 codec g711ulaw
```

Configure Crypto Authentication



Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure the preferred cipher-suites for the SRTP call leg (connection). For more information, see [Configure SRTP-SRTP Interworking](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Execute the commands based on your configuration mode
 - In dial-peer configuration mode:


```
dial-peer voice tag voip
voice-class sip srtp-auth {sha1-32 | sha1-80 | system}
```
 - In global VoIP SIP configuration mode:


```
voice service voip
sip
srtp-auth {sha1-32 | sha1-80}
```
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Execute the commands based on your configuration mode <ul style="list-style-type: none"> • In dial-peer configuration mode: <pre>dial-peer voice tag voip voice-class sip srtp-auth {sha1-32 sha1-80 system}</pre> • In global VoIP SIP configuration mode: <pre>voice service voip sip srtp-auth {sha1-32 sha1-80}</pre> Example: <pre>Device(config)# dial-peer voice 15 voip Device(config-dial-peer)# voice-class sip srtp-auth sha1-80</pre> Example: <pre>Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-serv-sip)# srtp-auth sha1-80</pre>	Configures an SRTP connection on CUBE using the preferred crypto suite. <ul style="list-style-type: none"> • The default value is sha1-32.
Step 4	end Example: Device(conf-serv-sip)# end	Ends the current configuration session and returns to privileged EXEC mode.

Example: Configuring Crypto Authentication



Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure the preferred cipher-suites for the SRTP call leg (connection). For more information, see [Configure SRTP-SRTP Interworking](#).

Example: Configuring Crypto Authentication (Dial Peer Level)

The following example shows how to configure CUBE to support an SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite at the dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 15 voip
Device(config-dial-peer)# voice-class sip srtp-auth sha1-80
Device(config-dial-peer)# end
```

Example: Configuring Crypto Authentication (Global Level)

The following example shows how to configure CUBE to support an SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp-auth sha1-80
Device(conf-serv-sip)# end
```

Enable SRTP Fallback

You can configure SRTP with the fallback option so that a call can fall back to RTP if SRTP is not supported by the other call end. Enabling SRTP fallback is required for supporting nonsecure supplementary services such as MoH, call forward, and call transfer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - In dial-peer configuration mode


```
dial-peer
voice
tag
voip

srtp
fallback (for interworking with devices other than Cisco Unified Communications Manager)
```

or

```
voice-class sip srtp
negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager )
```
 - In global VoIP SIP configuration mode

voice service voip

sip

srtp

fallback(for interworking with devices other than Cisco Unified Communications Manager)

or

srtp

negotiate cisco (Enable this CLI along with **srtp fallback** command to support SRTP fallback with Cisco Unified Communications Manager)

4. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • In dial-peer configuration mode <pre>dial-peer voice tag voip srtp fallback (for interworking with devices other than Cisco Unified Communications Manager) or voice-class sip srtp negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)</pre> <ul style="list-style-type: none"> • In global VoIP SIP configuration mode <pre>voice service voip sip</pre>	<p>Enables call fallback to nonsecure mode.</p>

	Command or Action	Purpose
	<p>srtp fallback(for interworking with devices other than Cisco Unified Communications Manager)</p> <p>or</p> <p>srtp negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)</p> <p>Example:</p> <pre>Device(config)# dial-peer voice 10 voip Device(config-dial-peer)# srtp fallback</pre> <p>Example:</p> <pre>Device(config)# dial-peer voice 10 voip Device(config-dial-peer)# voice-class sip srtp negotiate Cisco</pre> <p>Example:</p> <pre>Device(config)# voice service voip Device(config)# sip Device(conf-voi-serv)# srtp fallback</pre> <p>Example:</p> <pre>Device(config)# voice service voip Device(config)# sip Device(conf-voi-serv)# srtp negotiate cisco</pre>	
Step 4	<p>exit</p> <p>Example:</p> <pre>Device(conf-voi-serv)# exit</pre>	Exits present configuration mode and enters privileged EXEC mode.

Troubleshooting Tips

The following commands help in troubleshooting SRTP-RTP supplementary services support:

- **debug ccsip all**
- **debug voip ccapi inout**

Verify SRTP-RTP

Perform this task to verify the configuration for SRTP-RTP supplementary services support.

SUMMARY STEPS

1. **enable**
2. **show call active voice brief**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show call active voice brief

Displays call information for voice calls in progress.

Example:

```
Device# show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
ulticast call-legs: 0
Total call-legs: 4
0   : 1 12:49:45.256 IST Fri Jun 3 2011.1 +29060 pid:1 Answer 10008001 connected
dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
IP 10.45.40.40:7892 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0   : 2 12:49:45.256 IST Fri Jun 3 2011.2 +29060 pid:22 Originate 20009001 connected
dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
IP 10.45.40.40:7893 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0   : 3 12:50:14.326 IST Fri Jun 3 2011.1 +0 pid:0 Originate connecting
dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
IP 10.45.34.252:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0   : 5 12:50:14.326 IST Fri Jun 3 2011.2 +0 pid:0 Originate connecting
dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
IP 10.45.34.252:2000 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
```

```
media inactive detected:n media contrl rcvd:n/a timestamp:n/a  
long duration call detected:n long duration call duration:n/a timestamp:n/a
```



CHAPTER 61

SRTP-SRTP Pass-Through

- [Overview, on page 663](#)
- [Configure Pass-Through of Unsupported Crypto Suites for a Specific Dial Peer, on page 664](#)
- [Configure Pass-Through of Unsupported Crypto Suites Globally, on page 666](#)
- [Configuration Examples for SRTP-SRTP Pass-Through, on page 667](#)

Overview

SRTP-SRTP pass-through feature allows pass-through of encrypted media from one call-leg to the other.

Cisco Unified Border Element (CUBE) supports SIP calls between endpoints using Transport Layer Security (TLS) for SIP signaling encryption and Secure Real-Time Protocol (SRTP) to provide RTP media encryption. However, these two encryption mechanisms may not be deployed simultaneously, depending on the required call flow invoked on the associated configuration.

The following are conditions of the SRTP Passthrough feature:

- SRTP Passthrough must be configured on both legs of the call. If the target adjacency does not support SRTP Passthrough, then the call is rejected by error message 415 (Unsupported Media Type).
- "m= .. RTP/SAVP .." and a="crypto:..." fields coming in on an Invite from one adjacency are passed on in an Invite to the target adjacency.
- "m= ...RTP/SAVP..." is a required field in the Invite to trigger SRTP Passthrough behavior in the CUBE.

Pass-Through of Unsupported Crypto Suites



Note Effective from Cisco IOS XE Everest Release 16.5.1b, CUBE supports AEAD_AES_128_GCM and AEAD_AES_256_GCM crypto-suites. For more information, see [SRTP-SRTP Interworking](#).

CUBE supports transparent passthrough of all (supported and unsupported) crypto suites.

CUBE has the ability to pass across crypto attributes (containing any unsupported crypto suites) as well as media packets (encrypted with unsupported crypto suites).

If SRTP pass-thru feature is enabled, media interworking will not be supported. Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Feature Information

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 85: Feature Information for SRTP-SRTP Pass-Through

Feature Name	Releases	Feature Information
Support for SRTP-SRTP Basic calls	Baseline functionality	This feature introduced support for basic SRTP-SRTP pass-through calls.

Configure Pass-Through of Unsupported Crypto Suites for a Specific Dial Peer

SUMMARY STEPS

1. **enable**
2. configure terminal
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *string*
5. **session protocol sipv2**
6. **sessiontarget ipv4:** *destination-address*
7. **incoming called-number** *string*
8. **srtp pass-thru**
9. **codec** *codec*
10. **end**
11. **dial-peer voice** *tag* **voip**
12. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
13. **srtp pass-thru**
14. **codec** *codec*
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: Device(config)# <code>dial-peer voice 201 voip</code>	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> • In the example, the following parameters are set: <ul style="list-style-type: none"> • Dial peer 201 is defined. • VoIP is shown as the method of encapsulation.
Step 4	destination-pattern string Example: Device(config-dial-peer)# <code>destination-pattern 5550111</code>	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. <ul style="list-style-type: none"> • In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	session protocol sipv2 Example: Device(config-dial-peer)# <code>session protocol sipv2</code>	Specifies a session protocol for calls between local and remote routers using the packet network. <ul style="list-style-type: none"> • In the example, the sipv2 keyword is configured so that the dial peer uses the IETF SIP.
Step 6	sessiontarget ipv4: destination-address Example: Device(config-dial-peer)# <code>session target ipv4:10.13.25.102</code>	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer. <ul style="list-style-type: none"> • In the example, the IP address of the dial peer to receive calls is configured as 10.13.25.102.
Step 7	incoming called-number string Example: Device(config-dial-peer)# <code>incoming called-number 5550111</code>	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. <ul style="list-style-type: none"> • In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	srtp pass-thru Example: Device(config-dial-peer)# <code>srtp pass-thru</code>	Enables transparent passthrough of all crypto suites for a specific dial peer.
Step 9	codec codec Example: Device(config-dial-peer)# <code>codec g711ulaw</code>	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.

	Command or Action	Purpose
Step 10	end Example: Device(config-dial-peer)# end	Exits dial peer voice configuration mode.
Step 11	dial-peer voice tag voip Example: Device(config)# dial-peer voice 200 voip	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> • In the example, the following parameters are set: <ul style="list-style-type: none"> • Dial peer 200 is defined. • VoIP is shown as the method of encapsulation.
Step 12	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 13	srtp pass-thru Example: Device(config-dial-peer)# srtp pass-thru	Enables transparent passthrough of all crypto suites for a specific dial peer.
Step 14	codec codec Example: Device(config-dial-peer)# codec g711ulaw	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 15	exit Example: Device(config-dial-peer)# exit	Exits dial peer voice configuration mode.

Configure Pass-Through of Unsupported Crypto Suites Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **srtp pass-thru**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	srtp pass-thru Example: Device(config-dial-peer)# srtp pass-thru	Enables transparent passthrough of all crypto suites globally.
Step 5	end Example: Device(config-dial-peer)# end	Exits dial peer voice configuration mode.

Configuration Examples for SRTP-SRTP Pass-Through

Example for SRTP=SRTP Pass-Through

```

enable
configure terminal
dial-peer voice 201 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.102
incoming called-number 5550111
srtp
codec g711ulaw
end

dial-peer voice 200 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.101
incoming called-number 5550111
srtp
codec g711ulaw
end

```

Example for Pass-Through of Unsupported Crypto Suites for a specific dial peer

```
enable
configure terminal
dial-peer voice 201 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.102
incoming called-number 5550111
srtp pass-thru
codec g711ulaw
end
```

```
dial-peer voice 200 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.101
incoming called-number 5550111
srtp pass-thru
codec g711ulaw
end
```

Example for Pass-Through of Unsupported Crypto Suites Globally

```
enable
configure terminal
voice service voip
srtp pass-thru
end
```



CHAPTER 62

Monitoring of Phantom Packets

- [Overview, on page 669](#)
- [Restrictions, on page 670](#)
- [Configure Monitoring of Phantom Packets, on page 670](#)
- [Configuration Examples for Monitoring of Phantom Packets, on page 672](#)
- [Additional References for Configurable Pass-Through of SIP INVITE Parameters, on page 672](#)

Overview

The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. This allows the VoIP RTP layer to safely drop packets without proper sessions (phantom packets) received on these ports of the Cisco Unified Border Element (CUBE) or Voice time-division multiplexing (TDM) gateways. Because the ports are configured specifically for the VoIP RTP layer, punting the packets to UDP process is not required. This helps in reducing the performance issues.

The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. This configuration allows the VoIP RTP layer to safely drop packets without proper sessions (phantom packets) received on the ports of the Cisco Unified Border Element (CUBE) or Voice time-division multiplexing (TDM) gateways. Because the ports are configured specifically for the VoIP RTP layer, there is no need to punt the packets to the UDP process in case the packets were intended for some other application, thus reducing performance issues.

A phantom packet is a valid RTP packet meant for the CUBE or Voice TDM gateway without an existing session on the respective gateways. When a phantom packet is received by the VoIP RTP layers of the gateways, the packet is punted to the UDP process to check if it is required by any other applications causing performance issues, especially when a large number of such packets are received. A malicious attacker can also send a large number of phantom packets. The packet is punted to the UDP process because UDP port ranges are shared by many applications other than VoIP RTP and the VoIP RTP layer cannot drop the packet assuming the packet is for itself.

It is recommended that you configure the IP address and port ranges specific to the media IP addresses, even if you are using a single virtual IP address for media. This feature allows you to configure port ranges specific to the VoIP RTP layer. If a phantom packet is received on the configured port, the VoIP RTP layer can safely drop the packet. If a phantom packet is received on any other port, the VoIP RTP layer punts the packet to the UDP process.

Feature Information

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 86: Feature Information for Monitoring of Phantom Packets

Feature Name	Releases	Feature Information
Monitoring of Phantom Packets	Baseline functionality	This feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer and drop phantom RTP packets (RTP packets that are configured in valid port range but for which there is no matching call or session).

Restrictions

- The authentication, authorization, and accounting (AAA) default port range of 21645–21844 must not be configured.
- Up to ten port range entries can be defined under a single media-address range.
- The minimum port must be numerically lower than the maximum port.
- Port ranges should not overlap.
- Address ranges should not overlap.
- Address ranges and single addresses should not overlap.
- Where a range of addresses are defined in a single command, they share any port ranges assigned. If there is a requirement to have different port ranges for different media addresses, then the addresses must be configured separately.

Configure Monitoring of Phantom Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media-address range** *starting-ip-address ending-ip-address* **port range** *starting-port-number ending-port-number*

5. `port-range starting-port-number ending-port-number`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Specifies VoIP encapsulation and enters voice-service configuration mode.
Step 4	media-address range <i>starting-ip-address ending-ip-address</i> port range <i>starting-port-number ending-port-number</i> Example: Using IPv4 addresses: For single IP: Device(conf-voi-serv)# media-address range 10.1.1.1 10.1.1.1 For a range of IPs: Device(conf-voi-serv)# media-address range 10.1.1.1 10.1.1.254 Example: Using IPv6 addresses: For single IP: Device(conf-voi-serv)# media-address range 2001:DB8:1::1 2001:DB8:1::1 For a range of IPs: Device(conf-voi-serv)# media-address range 2001:DB8:1::1 2001:DB8:1::17 Example: Port range for media address. Device(cfg-media-addr-range)# port-range 8000 48198	Configures an IPv4 or IPv6 media address range. And, creates a port range for the configured media addresses. Note If you do not configure any port range, the default port range is applied. The default port range is 8000-48198 for ASR and ISR G3 platforms.
Step 5	port-range <i>starting-port-number ending-port-number</i> Example:	Configures a port range. If you do not configure any port range nothing is applied.

	Command or Action	Purpose
	Device (cfg-media-addr-range) # port-range 8000 48198	Note Ensure that the port range is not greater than the port range (if configured) specified in the media-address range command.
Step 6	end Example: Router (cfg-media-addr-range) # end	Exits voice-service configuration mode and returns to privileged EXEC mode.

Configuration Examples for Monitoring of Phantom Packets

```

Device (config) # voice service voip
Device (conf-voi-serv) # media-address range 10.1.1.1 10.1.1.254
Device (cfg-media-addr-range) # port-range 8000 21643
Device (cfg-media-addr-range) # port-range 21846 48000
Device (cfg-media-addr-range) # exit

Device (conf-voi-serv) # media-address range 2001:DB8:1::1 2001:DB8:1::17
Device (cfg-media-addr-range) # port-range 8000 21643
Device (cfg-media-addr-range) # port-range 21846 48000
Device (cfg-media-addr-range) # end

```



Note The ports 21643–21845 are not used by the RTP layer. They might be used by applications such as AAA/Radius. These ports are allowed to be punted to the control plane if needed.

Additional References for Configurable Pass-Through of SIP INVITE Parameters

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS commands	Cisco IOS Command List, All Releases
SIP configuration tasks	SIP Configuration Guide, Cisco IOS Release 15M&T

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/support</p>



CHAPTER 63

Security Compliance

- [Overview, on page 675](#)
- [Supported Hardware and Software for Virtual CUBE, on page 676](#)
- [Common Criteria Configuration on Cisco CSR 1000v and C8000v, on page 676](#)
- [FIPS Configuration on Cisco CSR 1000v and C8000v, on page 688](#)

Overview

Cisco Unified Border Element (CUBE) is Common Criteria (CC) and The Federal Information Processing Standards (FIPS) certified. The certification is applicable to CUBE on Cisco CSR 1000v/Cisco CSR 8000v platform only.

Common Criteria (CC)

Common Criteria (CC) is a global security standard to which security products are evaluated. Common Criteria product certifications are mutually recognized by 28 nations, thus an evaluation that is conducted in one country is recognized by the other countries.

The Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) that guarantees product security. The organizations (Government or Enterprise IT) specify functional and assurance requirements, the vendors claim and develop specific product qualities. The testing facilities examine products to determine whether they meet those vendor claims. Common Criteria guarantees that the process of specification, execution and assessment of a product has been conducted in a stringent and standardized manner.

The Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module should be a set of hardware, software, firmware, or some combination that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain crypto algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

Feature Information

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 87: Feature Information

Feature Name	Releases	Feature Information
Common Criteria (CC) and The Federal Information Standards (FIPS) Certification.	Cisco IOS XE Fuji Release 16.9.1	Common Criteria (CC) and The Federal Information Standards (FIPS) Certification for CUBE on Cisco CSR 1000v.

Supported Hardware and Software for Virtual CUBE

For details on prerequisites for Virtual CUBE, see [Supported Hardware and Software for Virtual CUBE](#).

Common Criteria Configuration on Cisco CSR 1000v and C8000v

Enable Common Criteria Mode

Before you begin

- Delete existing certificates.
- Remove existing crypto keys.
- Remove existing TLS configuration (TLS version and Cipher Suites).

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 **cc-mode****Example:**

```
Router(config)# cc-mode
```

Enables common criteria configuration mode.

What to do next

Common Criteria (CC) mode enforces certain security checks for cryptographic protocols such as Transport Layer Security (TLS). CUBE uses TLS to secure signaling over SIP and HTTP client for XCC providers. Configure SIP TLS and HTTP TLS in the Common Criteria (CC) mode.

SIP TLS Configuration

SIP TLS Configuration Task Flow

Following are the steps to configure SIP TLS on your Cisco CSR 1000v router in Common Criteria mode.

1. [Generate RSA Public Key, on page 677](#)
2. [Configure Certificate Authority Server, on page 678](#)
3. [Configure CSR Trustpoint, on page 679](#)
4. [Configure Peer Trustpoint, on page 680](#)
5. [Add Client Verification Trustpoint, on page 681](#)
6. [Enforce Strict SRTP, on page 682](#)

Generate RSA Public Key

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 **crypto key generate rsa label** *key-label* **modulus** *modulus-size*

Example:

```
Router(config)#crypto key generate rsa general-keys label CUBE modulus 3072
```

Generates a public RSA key that is used with your CSR certificate.

- The *key-label* specifies the name that is used for an RSA key pair when they are exported.
- The *modulus-size* specifies the size of the key modulus. By default, the modulus of a Certification Authority (CA) key is 1024 bits. The size of the key modulus must be 2048 bits or higher, for it to be Common Criteria compliant.

Step 4 **exit****Example:**

```
Router(config)#exit
```

Exits global configuration mode.

Configure Certificate Authority Server

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 **crypto pki server *cs-label*****Example:**

```
Router(config)# crypto pki server CUBE
```

Defines a label for the Certificate Server and enters the certificate server configuration mode.

Note If you have generated the RSA key pair manually using the command **crypto key generate rsa label *key-label* modulus *modulus-size***, the *cs-label* must match with the *key-label*, otherwise a certificate with the default key size of 1024 bits is generated.

Step 4 **database level complete****Example:**

```
Router(cs-server)# database level complete
```

Writes each issued certificate to the certificate enrollment database.

Step 5 **grant auto**

Example:

```
Router(cs-server)# grant auto
```

Automatically grants reenrollment requests for subordinate Certificate Authority (CA) server or Registration Authority (RA) mode Certificate Authority (CA).

Step 6 hash sha384**Example:**

```
Router(cs-server)# hash sha384
```

Sets the hash function SHA-384 for the signature that the Cisco IOS Certificate Authority (CA) uses to sign all the certificates that are issued by the server.

Step 7 no shut**Example:**

```
Router(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password:

Re-enter password:

% Generating 3072 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.
```

Enables or reenables the certificate server. If the subordinate certificate server is enabled for the first time, the certificate server generates the key and receives its signing certificate from the root certificate server.

After entering the passphrase (when prompted), the certificate server is enabled. This passphrase protects the private key.

Step 8 exit**Example:**

```
Router(cs-server)# exit
```

Exits certificate server configuration mode.

Configure CSR Trustpoint

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 **crypto pki trustpoint** *name***Example:**

```
Router(config)#crypto pki trustpoint CUBE-TLS
```

Declares the trustpoint with the name specified and enters trustpoint configuration mode. This trustpoint is used by your Router application for the TLS communication.

Step 4 **hash sha384****Example:**

```
Router(ca-trustpoint)#hash sha384
```

Sets the hash function SHA-384 for the signature that the Cisco IOS Certificate Authority (CA) uses to sign all the certificates that are issued by the server.

A trustpoint with sample CSR certificate with subject-name "CN=Secure-Router" and "rsakeypair Router" is given below. The "rsakeypair label" must match with the label of the RSA keys that are generated in the earlier steps.

```
crypto pki trustpoint CUBE-TLS
 enrollment url http://X.X.X.X:80
 serial-number none
 fqdn none
 ip-address none
 subject-name CN=Secure-CUBE
 revocation-check none
 rsakeypair Router
```

Step 5 **exit****Example:**

```
Router(ca-trustpoint)# exit
```

Exits trustpoint configuration mode.

Configure Peer Trustpoint

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 **crypto pki trustpoint** *name***Example:**

```
Router(config)#crypto pki trustpoint xyzname
```

Declares the peer trustpoint with the name specified and enters trustpoint configuration mode.

Step 4 **enrollment terminal****Example:**

```
Router(ca-trustpoint)#enrollment terminal
```

Specifies manual certificate enrollment via the cut-and-paste method for trustpoint peers. The certificate request displayed on the console terminal can be manually copied.

Step 5 **revocation-check none****Example:**

```
Router(ca-trustpoint)#revocation-check none
```

Specifies that the certificate check is ignored.

Step 6 **exit****Example:**

```
Router(ca-trustpoint)#exit
```

Exits trustpoint configuration mode.

Add Client Verification Trustpoint

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 **sip-ua****Example:**

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

Enters SIP User Agent configuration mode to configure SIP-UA related commands.

Step 4 **crypto signaling remote-addr** *remote ip address remote ip mask* **trustpoint** *CUBE's trustpoint label* **client-vtp** *verification trustpoint*

Example:

```
Router(config-sip-ua)#crypto signaling remote-addr X.X.X.X 255.255.255.255 trustpoint CUBE-TLS
client-vtp CUBE-VERIFY
```

Assigns a client verification trustpoint to SIP-UA. This client verification trustpoint is used to send Distinguished Name (DN) of the Certificate Authority (CA) server in the CUBE's client certificate request.

Step 5 **exit**

Example:

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

Exits sip-ua configuration mode.

Enforce Strict SRTP

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 service voip**

Example:

```
Router(config)#voice service voip
```

Enters voice service configuration mode and specifies the encapsulation method as VoIP.

Step 4 **srtp**

Example:

```
Router(conf-voi-ser)#srtp
```

Enforces SRTP to secure the call flow through CUBE.

Step 5 **exit**

Example:

```
Router(conf-voi-ser)#exit
```

Exits voice service configuration mode.

HTTPS TLS Configuration

HTTPS TLS Configuration Task Flow

Following are the steps to configure HTTPS TLS on your Cisco CSR 1000v router in Common Criteria mode.

1. [Prepare Cisco CSR 1000v Router's HTTP Server to Run in CC Mode, on page 683](#)
2. [Create Certificate Map for HTTPS Peer Trustpoint, on page 684](#)
3. [Configure HTTPS TLS Version, on page 685](#)
4. [Configure Supported Cipher Suites, on page 686](#)
5. [Apply Certificate Map to HTTPS Peer Trustpoint, on page 686](#)

Prepare Cisco CSR 1000v Router's HTTP Server to Run in CC Mode

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 **ip http server *name***

Example:

```
Router(config)#ip http server
```

Enables the HTTP server on the Cisco CSR 1000v router, allowing the use of Cisco web browser UI to monitor the router and issue commands to it.

Step 4 **ip http authentication local**

Example:

```
Router(config)#ip http authentication local
```

Specifies the authentication method for HTTP server users. The keyword **local** indicates that the username, password, and privilege level access combination that is specified in the local system configuration should be used for authentication and authorization.

Step 5 **ip http secure-server****Example:**

```
Router(config)#ip http secure-server
```

Enables a secure HTTP server on the Cisco CSR 1000v router.

Step 6 **ip http secure-trustpoint** *trustpoint-name***Example:**

```
Router(config)#ip http secure-trustpoint CUBE-TLS
```

Specifies the trustpoint that is used for obtaining signed certificates for a secure HTTP server on the Cisco CSR 1000v router.

Step 7 **ip http secure-client-auth****Example:**

```
Router(config)#ip http secure-client-auth
```

Configures the HTTP server to request an X.509v3 certificate from the client to authenticate the client during the connection process.

Step 8 **ip http secure-peer-verify-trustpoint** *client's issuer***Example:**

```
Router(config)#ip http secure-peer-verify-trustpoint secure-clientissuer
```

Configures the client verification trustpoint for the HTTP server on the Cisco CSR 1000v router. This peer verification trustpoint is used to send Distinguished Name (DN) of Certificate Authority (CA) in the client certificate request during the TLS handshake of HTTP.

Step 9 **exit****Example:**

```
Router(config)#exit
```

Exits the global configuration mode.

Create Certificate Map for HTTPS Peer Trustpoint

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 **crypto pki certificate map** *label sequence-number*

Example:

```
Router(config)#crypto pki certificate map cubemap 10
```

Creates a certificate map that defines certificate-based Access Control Lists (ACLs) and enters the certificate map configuration mode. The *sequence-number* orders the ACLs with the same label. ACLs with the same label are processed from the lowest to the highest sequence number. When an ACL is matched, the processing stops with a successful result.

Step 4 **alt-subject-name eq** *match-value*

Example:

```
Router(ca-certificate-map)#alt-subject-name peername
```

Specifies the certificate fields with their matching criteria in the certificate map configuration mode. The alternate subject name that is specified in the map must be present in SAN extension of the peer id certificate.

Step 5 **exit**

Example:

```
Router(ca-certificate-map)#exit
```

Exits certificate map configuration mode.

Configure HTTPS TLS Version

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 **ip http tls-version** *version*

Example:

```
Router(config)#ip http tls-version TLSv1.2
```

Configures the specified TLS version for HTTPS. Configure TLSv1.1 or TLSv1.2 to be Common Criteria compliant.

Step 4 **exit**

Example:

```
Router(config)#exit
```

Exits global configuration mode.

Configure Supported Cipher Suites

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 ip http secure-ciphersuite *supported cipher suites*

Example:

```
Router(config)#ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha  
rsa-aes-cbc-sha2 rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2  
ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
```

Specifies the cipher suites that are used for encryption over the secure HTTP connection between the client and the HTTP server. Common Criteria supports the cipher suites that are given in the preceding example. Configure all the cipher suites if you are not aware of the client cipher support.

Step 4 exit

Example:

```
Router(config)#exit
```

Exits global configuration mode.

Apply Certificate Map to HTTPS Peer Trustpoint

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 `crypto pki trustpoint name`**Example:**

```
Router(config)#crypto pki trustpoint CUBE-HTTPS
```

Declares the HTTPS peer trustpoint for the Cisco CSR 1000v router.

Step 4 `match certificate map name`**Example:**

```
Router(ca-trustpoint)#match certificate cubemap
```

Associates the certificate map that is defined by using the **crypto pki certificate map** command with the HTTPS trustpoint. The *map name* argument in the **match certificate** command must match the *label* argument that is specified in the previously defined **crypto pki certificate map** command.

Step 5 `match eku attribute`**Example:**

```
Router(ca-trustpoint)#match eku client-auth server-auth
```

Allows the HTTPS peer which acts as a client and a server to validate a peer certificate only if the specified Extended Key Usage (EKU) attribute is present in the certificate. If the Cisco CSR 1000v router is a client, then you must configure server-auth. If Cisco CSR 1000v router is a server, then you must configure client-auth.

Step 6 `exit`**Example:**

```
Router(ca-trustpoint)#exit
```

Exits trustpoint configuration mode.

NTP Configuration Restrictions in Common Criteria Mode

In Common Criteria mode, the following restrictions are applicable to NTP configuration.

- Do not configure NTP version 1 and 2. Following are the NTP version commands.
 - **ntp server ip-address prefer source interface version version**
 - **ntp peer ip-address version version**
- Do not configure NTP broadcast. Following are the NTP broadcast commands.
 - **ntp broadcast delay delay-timer**
 - **ntp broadcast client**
 - **ntp broadcast destination ip-address**
 - **ntp broadcast destination ip-address key key**

- **ntp broadcast destination** *ip-address* **key** *key* **version** *version*
- **ntp broadcast version** *version*
- Do not configure NTP multicast command **ntp multicast version** *version*.

FIPS Configuration on Cisco CSR 1000v and C8000v

Configuration Requirements for FIPS Compliance

There is no specific command to enable FIPS mode. For the Virtual CUBE on the Cisco CSR 1000v router to be FIPS-compliant, the following commands must be configured.

- **crypto key generate rsa modulus** *modulus-size*
The *modulus-size* varies from 360 bits to 4096 bits. The size of the RSA key must be 2048 bit or higher for FIPS compliance.
- The Hash Algorithms that are configured using the command **hash sha384** under the configured trustpoint and the crypto pki server on the CSR must use sha384 or greater, namely sha512.



PART **X**

Configure Multiple Trunks Using Tenants

- [Configure Multiple Trunks Using Tenants](#) , on page 691
- [Support for Multi VRF](#) , on page 701



CHAPTER 64

Configure Multiple Trunks Using Tenants

- [Overview, on page 691](#)
- [Configure SIP Trunks using Voice Class Tenant, on page 696](#)

Overview

The CUBE Tenant feature allows you to configure SIP trunks individually using parameters that were previously only available globally, or with individual dial-peers. Tenants act as a configuration template for dial-peers, which allow you to customize the global configuration to suit the requirements for each trunk. Dial-peers associated with a tenant automatically receive all of its configuration, making trunk configuration simple and consistent. If necessary, specific configurations may be overridden at the dial-peer level, allowing maximum flexibility.

When bound to an interface configured with a VRF, the tenant feature may also be used to configure trunks for multiple customers, each with their own characteristics on the same platform.

The **voice class tenant** *<tag>* command allows sip-specific attributes to be configured for each trunk. The command **voice class tenant** *<tag>* can then be used to apply the tenant configuration to individual dial-peers. Refer to "[Table 88: Multi-Tenant Configuration List, on page 692](#)" for information on the complete list of configurations present under the **voice class tenant** *<tag>*.

If tenants are configured under dial-peer, then configurations are applied in the following order of preference.

- Dial-peer configuration
- Tenant configuration
- Global configuration

That is, if the value of the attribute under dial-peer configuration is system, then the value is taken from the tenant configuration. And, if the value under the tenant configuration is also system, then the global configuration is used.

If there are no tenants configured under dial-peer, then the configurations are applied using the default behavior in the following order:

- Dial-peer configuration
- Global configuration

The following table lists the various configurations present under **voice class tenant** <tag>. For more information on specific configurations, see the [Voice and Video](#) command reference guide lists.



Note Attributes that are not available under **voice class tenant** <tag> use the default behavior—With preference of dial-peer followed by the global configuration.

Table 88: Multi-Tenant Configuration List

Command	Description
aaa	SIP-UA AAA related configuration
anat	Allow alternative network address types IPv4 and IPv6
asserted-id	Configure SIP UA privacy identity settings
associate	Associate a RCB for outgoing calls
asymmetric	Configure global SIP asymmetric payload support
authentication	Digest Authentication Configuration
bandwidth	Allow SIP SDP bandwidth-related options
bind	SIP bind command
block	Block 18X response to INVITE
call-route	Configure call routing options
conn-reuse	Reuse the sip registration tcp connection for the end-point behind a Firewall
connection-reuse	Use listener port for sending requests over UDP
contact-passing	302 contact to be passed through for CFWD
content	Content carried as part of SIP message
copy-list	Configure list of entities to be sent to peer leg
credentials	User credentials for registration
disable-early-media	Disable early-media cut through
dns -a-override	Skip DNS A/AAAA query when SRV query timeout
dscp -profile	DSCP Profile global config
early-media	Configure method to handle early-media Update Request
early-offer	Configure sending Early-Offer

Command	Description
encap	Configure SDP encapsulation
error-code-override	Configure sip error code
error- passthru	SIP error response pass-thru functionality
exit	Exits from the voice class configuration mode
g729	G729 codec interoperability settings
handle-replaces	Handle INVITE with REPLACES header at SIP spi
header-passing	SIP Headers need to be passed to applications
help	Description of the interactive help system
history-info	History Info header support
host-registrar	Use sip-ua registrar value in Diversion and Contact header for 3xx messages
interop-handling	Enable interop-handling
localhost	Specify the DNS name for the localhost
map	Mapping options
max-forwards	Change number of max-forwards for SIP Methods
midcall -signaling	Configure method to handle mid-call signaling
nat	SIP nat global config
no	Negate a command or set its defaults
notify	SIP Signaling Notify Configuration
offer	Configure settings for Offers made from the Gateway
options-ping	Send OPTION pings to remote end
outbound-proxy	Configure an Outbound Proxy Server
pass-thru	SIP pass-through global config
permit	Permit hostname for this gateway
preloaded-route	Use pre-loaded route header for outgoing calls, if available
privacy	Configure SIP UA privacy settings
privacy-policy	Set privacy behavior for outgoing SIP messages

random-contact	Use Random Contact for outgoing calls, if available
random-request- uri	Configure options for Request-URI having random value
reason-header	Configure settings for supporting SIP Reason Header
redirection	Enable call redirection (3xx) handling
refer- ood	Configure maximum number of out-of-dialog refer made to the Gateway
referto -passing	Refer-To needs to be passed through for transfer
registrar	Configure SIP registrar VoIP Interface
registration	Enable registration options
rellxx	Type of reliable provisional response support
remote-party-id	Enable Remote-Party-ID support in SIP User Agent
requi -passing	Request URI needs to be passed through
reset	SIP Reset Options
retry	Change default retries for each SIP Method
send	Configure outgoing message options
session	SIP Voice Protocol session config
sip-profiles	SIP Profiles global config
sip-server	Configure a SIP Server Interface
srtp	Allow SIP related SRTP options
srtp-auth	Allow to set preferred suites
tel-config	Tel format cfg for headers other than req -line in
timers	SIP Signaling Timers Configuration
update- callerid	Enable sending updates for callerid
url	Url configuration for request-line url in outgoing INVITE
video	Video related config for sip
warn-header	SIP Warning-Header global config

Feature Information

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 89: Feature Information

Feature Name	Releases	Feature Information
Support for Configuring Multi Tenants on SIP Trunk	Cisco IOS 15.6(2)T Cisco IOS XE Denali 16.3.1	This feature allows the provision to configure specific global configurations for multiple tenants on SIP trunks. The following commands were introduced: voice class tenant tag and voice-class sip tenant tag .

Feature Characteristics of Configurable SIP Trunk Listen Port

- For Cisco IOS XE Cupertino 17.8.1a and later releases, you can also configure a listen-port at the tenant level. Before this release, you could configure the listen-port only at the global configuration level.
- Multiple inbound TLS, TCP, or UDP connections can be established using different IP ports. Each port is mapped to a tenant trunk configuration, which may have its own TLS profile validation criteria.
- A tenant listen port may only be configured when there are no active calls on associated dial-peers.
- Tenant level listen-port configuration is supported for both secure (TLS) and nonsecure (TCP/UDP) transport types.
- Interface binding must be configured for a tenant to use a SIP trunk listen port.
- IPv4 and IPv6 listen ports may be configured for TLS, TCP or UDP transport types.
- The listen-port along with the bind interface must be unique across all:
 - Global and tenant level configuration modes
 - Secure and nonsecure ports
- If you modify the interface to which a tenant is bound, the existing listen-port will be closed and re-opened with the latest interface details.
- When there is a configuration change at the **bind** or **tenant level**, all the associated active connections are closed.
- The nonsecure listen-port range is limited to 5000 - 5500 to avoid overlap with the RTP port range, especially for UDP.

- Connections get segregated at the tenant level during inbound dial-peer matching. For this, the tenant tag in the inbound dial-peer is matched with the tenant tag that is identified during connection establishment.

To use the SIP trunk listen port feature, must configure the associated tenant with a SIP listen port:

- **tls-profile** *<tag>* under **voice class tenant** *tag* configuration mode.

For more information on the CLI commands, see [Cisco IOS Voice Command Reference Guide](#).

Feature Characteristics of Trunk Specific TLS Policy

- For TLS connections, the trustpoint selection is as follows:
 - The trustpoint is selected based on tenant configuration.
 - If this is not available, then the remote-IP or global configurations are used.



Note Except for the CN-SAN certificate validation, CUBE retains the same behavior for inbound nonsecure connections (TCP and UDP transport types).

To use a trunk specific TLS policy, you must configure the associated tenant with a TLS policy:

- **listen-port** { **non-secure** *port-number* | **secure** *port-number* } under **voice class tenant** *tag* configuration mode.

For more information on the CLI commands, see [Cisco IOS Voice Command Reference Guide](#).

Configure SIP Trunks using Voice Class Tenant

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Use the following to configure trunks using the tenant feature:
 - **voice class tenant** *<tag>* in the global configuration mode

Once you configure the **voice class tenant** *<tag>* command in the global mode, the configuration will move to the **voice class tenant** *<tag>* submode. You can configure all the sip-specific attributes in this submode.

 - **voice-class sip tenant** *<tag>* in the dial-peer configuration mode
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>Use the following to configure trunks using the tenant feature:</p> <ul style="list-style-type: none"> • voice class tenant <tag> in the global configuration mode <p>Once you configure the voice class tenant <tag> command in the global mode, the configuration will move to the voice class tenant <tag> submode. You can configure all the sip-specific attributes in this submode.</p> <ul style="list-style-type: none"> • voice-class sip tenant <tag> in the dial-peer configuration mode <p>Example:</p> <p>In global configuration mode</p> <pre>! Configuring tenant 1 Device(config)# voice class tenant 1 Device (config-class)# ? aaa - sip-ua AAA related configuration anat - Allow alternative network address types IPV4 and IPV6 asserted-id - Configure SIP-UA privacy identity settings Video - video related function Warn-header - SIP related config for SIP. SIP warning-header global config. Device (config-voi-tenant)# end ----- ! Configuring tenant 2 Device(config)# voice class tenant 2 Device (config-class)# ? aaa - sip-ua AAA related configuration anat - Allow alternative network address types IPV4 and IPV6 asserted-id - Configure SIP-UA privacy identity settings outbound-proxy - Configure an Outbound Proxy Server pass-thru - SIP pass-through global config</pre>	<p>Use the voice-class sip tenant <tag> command in the global configuration mode to configure a tenant with sip-specific attributes. This command tag can then be applied to one or more dial-peers using the voice-class sip tenant <tag> command under the dial-peers.</p>

Example: Multiple Trunks using Registration with Tenants

	Command or Action	Purpose
	<pre> srtp - Allow SIP related SRTP options Warn-header - SIP related config for SIP. SIP warning-header global config. Device (config-voi-tenant)# end Example: In dial-peer configuration mode !Configuring tenant 1 under dial-peer 10 Device (config)# dial-peer voice 10 voip Device (config-dial-peer)# voice-class sip tenant 1 Device (config-dial-peer)# end ----- !Configuring tenant 2 under dial-peer 20 Device (config)# dial-peer voice 20 voip Device (config-dial-peer)# voice-class sip tenant 2 Device (config-dial-peer)# end !An example for the use of the "no" form of command voice-class sip tenant Router(config)# dial-peer voice 3000 voip Router(config-dial-peer)# voice-class sip tenant 1 Router(config-dial-peer)# no voice-class sip tenant 1 When the no form is configured, the dial-peer is no longer associated with the tenant tag configuration. The attributes are now applied using the default order of dial-peer followed by the global configuration. </pre>	
Step 4	<pre> end Example: Device(config-dial-peer)# end </pre>	Returns to privileged EXEC mode.

Example: Multiple Trunks using Registration with Tenants

Trunk registration details may also be included in a tenant configuration, allowing a platform to register to multiple registrars concurrently. Tenants configured with registration details do not need to be associated with a dial-peer for the registration process to start.

```
Router# show run | sec tenant
```

```

Voice class tenant 1
registrar 1 ipv4:10.64.86.35:9051 expires 3600
credentials username aaaa password 7 06070E204D realm aaaa.com
outbound-proxy ipv4:10.64.86.35:9057
bind control source-interface GigabitEthernet0/0

```

```

Voice class tenant 2
registrar 1 ipv4:9.65.75.45:9052 expires 3600
credentials username bbbb password 7 110B1B0715 realm bbbb.com

```

```
outbound-proxy ipv4:10.64.86.40:9040
bind control source-interface GigabitEthernet0/1
```

For multi-tenancy support on Cisco Unified Border Element, you can configure voice class tenants with different credentials, but having the same registrar. In that scenario, it is recommended that you configure the CLI commands **sip-server** and **registrar** under **voice class tenant** configuration. The following is a sample configuration:

```
voice class tenant 1
  credentials number 1111 username test password 7 071B245B5D1D realm ipvoice.jp
  authentication username test password 7 06120A3258
  registrar ipv4:1.1.1.1 expires 120
  sip-server ipv4:1.1.1.1
!
voice class tenant 2
  credentials number 2222 username test password 7 09584B1E0A11 realm ipvoice.jp
  authentication username test2 password 7 071B245F5A
  registrar ipv4:1.1.1.1 expires 120
  sip-server ipv4:1.1.1.1
```

Example: Multiple Trunks using Registration with Tenants



CHAPTER 65

Support for Multi VRF

- Overview , on page 701
- Restrictions, on page 703
- Recommendations, on page 704
- Configure VRF, on page 704
- Configure VRF Specific RTP Port Ranges, on page 710
- Directory Number (DN) Overlap across Multiple-VRFs , on page 713
- IP Overlap with VRF, on page 715
- Use Server Groups with VRF, on page 717
- Inbound Dial-Peer Matching Based on Multi-VRF, on page 718
- VRF Aware DNS for SIP Calls, on page 720
- High Availability with VRF, on page 720
- Configuration Examples, on page 721
- Troubleshooting Tips, on page 731

Overview

The Virtual Routing and Forwarding (VRF) feature allows Cisco Unified Border Element (CUBE) to have multiple instances of routing and forwarding table to co-exist on the same device at the same time.

With Multi-VRF feature, each interface or subinterface can be associated with a unique VRF.



Note The information in this chapter is specific to Multi-VRF feature beginning in Cisco IOS Release 15.6(2)T. However, there is some information on Voice-VRF feature for the reference purpose only. For detailed information on the Voice-VRF feature, see http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t15/vrfawvgw.html.

Feature Information

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 90: Feature Information

Feature Name	Releases	Feature Information
Support for media flow-around using Multi-VRF	Cisco IOS XE Gibraltar 16.12.2	<p>This feature adds media flow-around support for the following intra-VRF call flows in standalone and high availability scenarios:</p> <ul style="list-style-type: none"> • Basic Audio Call • Call Hold and Resume • Re-INVITE based Call Transfer • 302 based Call Forward • Fax Pass Through Calls • T.38 Fax Calls <p>With media flow-around using Multi-VRF, only signalling is routed using VRFs and CUBE passes across the media IP and ports which it receives. For detailed information on media flow-around, see Media Path.</p>
Support up to 100 VRF instances	Cisco IOS XE Amsterdam 17.3.1	This feature enhancement provides support up to 100 VRFs. Each of the VRFs supports up to 10 different RTP port ranges.

Information About Voice-VRF

Support for Voice-VRF (also known as VRF-Aware) was introduced in Cisco IOS Release 12.4(11)XJ to provide support for configuring a VRF specific to voice traffic. Voice-VRF can be configured using **voice vrf vrf-name** command. For more information on voice-VRF, see http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t15/vrfawvgw.html.

Information About Multi-VRF

The Multi-VRF feature allows you to configure and maintain more than one instance of routing and forwarding tables within the same CUBE device and segregate voice traffic based on the VRF.

Multi-VRF uses input interfaces to distinguish calls for different VRFs and forms VRF tables by associating with one or more Layer 3 interfaces. Interface can be physical interface (such as FastEthernet ports, Gigabit Ethernet ports) or sub-interface. CUBE supports bridging calls on both intra-VRF and inter-VRF.



Note One physical interface or sub-interface can be associated with one VRF only. One VRF can be associated with multiple interfaces.

As per the Multi-VRF feature, the dial-peer configuration must include the use of the interface bind functionality. This is mandatory. It allows dial-peers to be mapped to a VRF via the interface bind.

The calls received on a dial-peer are processed based on the interface to which it is associated with. The interface is in turn associated with the VRF. So, the calls are processed based on the VRF table associated with that particular interface.

VRF Preference Order

Voice-VRF and Multi-VRF configurations can coexist. The following is the binding preference order for call processing:

Table 91: VRF Preference Order and Recommendations

Preference Order	Bind	Recommendations
1	Dial-peer Bind	—
2	Tenant Bind	Recommended for SIP trunk, especially when CUBE is collocated with Cisco Unified Survivability Remote Site Telephony. If Tenant bind is not configured, Voice-VRF is preferred for SIP trunk.
3	Global Bind	During device reboot, it is recommended to use global bind configuration to handle the early incoming traffic gracefully.
4	Voice-VRF	Recommended for hosted and cloud services configurations when CUBE is collocated with Cisco Unified Survivability Remote Site Telephony.

Restrictions

- Cisco Unified Communications Manager Express (Unified CME) and CUBE co-located with VRF is not supported.
- Cisco Unified Survivability Remote Site Telephony (Unified SRST) and CUBE co-location is not supported on releases before Cisco IOS XE Fuji 16.7.1.
- IPv6 on VRF is not supported.

- Calls are not supported when incoming dial-peer matched is default dial-peer (dial-peer 0).
- Media Anti-trombone is not supported with VRF.
- Cisco UC Services API with VRF is not supported.
- VRF aware matching is applicable only for inbound dial-peer matching and not for outbound dial-peer matching.
- Invoking TCL scripts through a dial-peer is not supported with the Multi-VRF.
- Multi-VRF using global routing table or default routing table (VRF 0) with virtual interfaces is not supported.
- Multi-VRF configured in media flow-around mode is supported only for intra-VRF calls. The following are not supported with Multi-VRF configured in media flow-around mode:
 - Supplementary services with REFER Consume, Mid-call (or Early Dialogue) block
 - Session Description Protocol (SDP) Passthrough
 - Media Recording
 - DSP flows (DTMF, transcode)

Recommendations

- For new deployments, we recommend a reboot of the router once all VRFs' are configured under interfaces.
- No VRF Route leaks are required on CUBE to bridge VoIP calls across different VRFs.
- High Availability(HA) with VRF is supported where VRF IDs are check-pointed in the event of fail-over. Ensure that same VRF configuration exists in both the HA boxes.
- Whenever destination server group is used with VRF, ensure that the server group should have the session targets, belonging to the same network as that of sip bind on the dial-peer, where the server-group is configured. This is because, dial-peer bind is mandatory with VRF and only one sip bind can be configured on any given dial-peer.
- If there are no VRF configuration changes at interface level, then reload of the router is not required.

Configure VRF



Note We recommend you NOT to modify VRF settings on the interfaces in a live network as it requires CUBE reload to resume VRF functionality.

This section provides the generic configuration steps for creating a VRF. For detailed configuration steps specific to your network scenario (Multi-VRF and Multi-VRF with HA), refer to Configuration Examples section.



Note You can also use the latest configuration option, which allows creation of multiprotocol VRFs that support both IPv4 and IPv6. Entering the command **vrf definition** *vrf-name* creates the multiprotocol VRF. Under VRF definition submenu, you can use the command **address-family** *{ipv4 | ipv6}* to specify appropriate address family. To associate the VRF with an interface, use the command **vrf forwarding** *vrf-name* under the interface configuration submenu.

For more information about the **vrf definition** and **vrf forwarding** commands, refer to the [Cisco IOS Easy Virtual Network Command Reference Guide](#).

Create a VRF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip vrf <i>vrf-name</i> Example: Device(config)# ip vrf <i>VRF1</i>	Creates a VRF with the specified name. In the example, VRF name is VRF1. Note Space is not allowed in VRF name.
Step 4	rd <i>route-distinguisher</i> Example: Device(config)# rd 1:1	Creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y)
Step 5	exit Example: Device(config)# exit	Exits present mode.

Assign Interface to VRF



Note If an IP address is already assigned to an interface, then associating a VRF with interface will disable the interface and remove the existing IP address. An error message (sample error message shown below) is displayed on the console. Assign the IP address to proceed further.

```
% Interface GigabitEthernet0/1 IPv4 disabled and address(es) removed due to
enabling VRF VRF1
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface***interface-name*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip address subnet mask*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-name</i> Example: Device(config)# interface <i>GigabitEthernet 0/1</i>	Enters the interface configuration mode.
Step 4	ip vrf forwarding <i>vrf-name</i> Example: Device(config-if)# ip vrf forwarding <i>VRF1</i>	Associates VRF with the interface. Note If there is an IP address associated with the interface, it will be cleared and you will be prompted to assign the IP address again.
Step 5	ip address <i>ip address subnet mask</i> Example: Device(config-if)# ip address <i>10.0.0.1 255.255.255.0</i>	IP address is assigned to the interface.

	Command or Action	Purpose
Step 6	exit Example: Device(config-if) # exit	Exits present mode.

Create Dial-peers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **session protocol** *protocol*
5. Create dial-peer:
 - To create inbound dial-peer:
incoming called number *number*
 - To create outbound dial-peer:
destination pattern *number*
6. **codec** *codec-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice <i>number</i> voip Example: Device(config)# dial-peer voice 1111 voip	Creates the dial-peer with the specified number.
Step 4	session protocol <i>protocol</i> Example: Device(config-dial-peer)# session protocol sipv2	Specifies the protocol associated with the dial-peer.

	Command or Action	Purpose
Step 5	Create dial-peer: <ul style="list-style-type: none"> To create inbound dial-peer: incoming called number <i>number</i> To create outbound dial-peer: destination pattern <i>number</i> Example: Inbound dial-peer: <pre>Device(config-dial-peer) # incoming called-number 1111</pre> Example: Outbound dial-peer: <pre>Device(config-dial-peer) # destination pattern 3333</pre>	Creates inbound and outbound dial-peer.
Step 6	codec <i>codec-name</i> Example: <pre>Device(config-dial-peer) # codec g711ulaw</pre>	Specifies the codec associated with this dial-peer.
Step 7	exit Example: <pre>Device(config-dial-peer) # exit</pre>	Exits present mode.

Bind Dial-peers

You can configure SIP binding at global level as well as at dial-peer level.

- Control and Media on a dial-peer have to bind with same VRF. Else, while configuring, the CLI parser will display an error
- Whenever global sip bind interface associated with a VRF is added,modified, or removed, you should restart the sip services under 'voice service voip > sip' mode so that the change in global sip bind comes into effect with associated VRF ID.

```
CUBE(config)# voice service voip
CUBE(conf-voi-serv) # sip
CUBE(conf-serv-sip) # call service stop
CUBE(conf-serv-sip) # no call service stop
CUBE(conf-serv-sip) # end
```

SUMMARY STEPS

- enable

2. **configure terminal**
3. Bind control and media to the interface
 - At dial-peer level:
 - dial-peer voice *number* voip**
 - voice-class sip bind control source-interface *interface-name***
 - voice-class sip bind media source-interface *interface-name***
 - At global configuration level
 - voice service voip**
 - sip**
 - bind control source-interface *interface-name***
 - bind media source-interface *interface-name***
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Bind control and media to the interface <ul style="list-style-type: none"> • At dial-peer level: <ul style="list-style-type: none"> dial-peer voice <i>number</i> voip voice-class sip bind control source-interface <i>interface-name</i> voice-class sip bind media source-interface <i>interface-name</i> • At global configuration level <ul style="list-style-type: none"> voice service voip sip bind control source-interface <i>interface-name</i> bind media source-interface <i>interface-name</i> Example:	Interface bind associates VRF to the specified dial-peer.

	Command or Action	Purpose
	<p>At dial-peer level:</p> <pre>Device(config)#dial-peer voice 1111 voip Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/1 Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/1</pre> <p>Example:</p> <p>At global configuration level:</p> <pre>Device(config)# voice service voip Device(conf-voi-serv)# sip Device(conf-voi-sip)# bind control source-interface GigabitEthernet0/1 Device(conf-voi-sip)# bind media source-interface GigabitEthernet0/1</pre>	
Step 4	<p>exit</p> <p>Example:</p> <pre>Device(config-dial-peer)# exit</pre>	Exits present mode.

Configure VRF Specific RTP Port Ranges

You can configure each VRF to have its own set of RTP port range for VoIP RTP connections under voice service voip. A maximum of ten VRF port ranges are supported. Different VRFs can have overlapping RTP port range. VRF based RTP port range limits (min, max port numbers) are same as global RTP port range. All three port ranges (global, media-address, VRF based) can coexist on CUBE and the preference order of RTP port allocation is as follows:

- VRF based port range
- Media-address based port range
- Global RTP port range

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media-address voice-vrf *vrf-name* port-range *min max***
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice service voip mode.
Step 4	media-address voice-vrf vrf-name port-range min max Example: Example 1 Device(conf-voi-serv)# media-address voice-vrf VRF1 port 16000 32000 The output: Device# show run section voice voice-card 0/3 dsp services dspfarm voice service voip no ip address trusted authenticate media-address voice-vrf VRF1 port 16000 32000 <i>*Here, the port-range is configured on the same line as the media address.</i> Example: Example 2 Device(conf-voi-serv)# media-address voice-vrf VRF1 Device(cfg-media-addr-vrf)# port-range 6000 7000 Device(cfg-media-addr-vrf)# port-range 8000 10000 Device(cfg-media-addr-vrf)# port-range 11000 20000 The output: Device# show run section voice voice-card 0/3 dsp services dspfarm voice service voip no ip address trusted authenticate media-address voice-vrf VRF1 port-range 6000 7000 port-range 8000 10000 port-range 11000 20000 <i>*In this case, multiple port range lines are configured under the media address.</i> Example: Example 3	Associates the RTP Port range with the VRF. If the RTP port range is not configured per each VRF, the default RTP port range is used across the VRFs used. You can configure up to ten port ranges per media address. The default port range is 8000-48198 for ASR and ISR G3 platforms. Note From Cisco IOS XE Amsterdam 17.3.1a onwards, you can configure 100 VRFs for up to 10 different RTP port ranges (that is, 10 different port ranges per each VRF).

Example: VRF with overlapping and non-overlapping RTP Port Range

	Command or Action	Purpose
	<p>CUBE supports up to 100 VRFs. Hence, you can configure up to 100 media address instances, that is, one instance per voice-vrf. This is subject to the maximum number of VRFs supported by the host platform.</p> <pre>Device(conf-voi-serv)# media-address voice-vrf VRF1 port-range 8000 48000 media-address voice-vrf VRF2 port-range 8000 48000 media-address voice-vrf VRF99 port-range 8000 48000 media-address voice-vrf VRF100 port-range 8000 48000</pre>	
Step 5	<p>exit</p> <p>Example:</p> <pre>Device(conf-voi-serv)# exit</pre>	Exits present mode.

Example: VRF with overlapping and non-overlapping RTP Port Range

Example 1 - Non-overlapping Port Range

The following is example shows two VRFs with non-overlapping RTP port range:

```
Device(conf)# voice service voip
Device(conf-voi-serv)# no ip address trusted authenticate
Device(conf-voi-serv)# media bulk-stats
Device(conf-voi-serv)# media-address voice-vrf vrf1 port-range 25000 28000
Device(conf-voi-serv)# media-address voice-vrf vrf2 port-range 29000 32000
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# redundancy-group 1
Device(conf-voi-serv)# sip
```

The output for command **show voip rtp connections** shows as follows:

```
Device# show voip rtp connections

VoIP RTP Port Usage Information:
Max Ports Available: 23001, Ports Reserved: 101, Ports in Use: 2

                                Min   Max   Ports   Ports
Ports
Media-Address Range              Port  Port  Available Reserved  In-use
-----
Global Media Pool                 8000  48198 19999      101      0
VRF ID Based Media Pool
-----
vrf1                              25000 28000 1501        0        1
vrf2                              29000 32000 1501        0        1
-----
VoIP RTP active connections :
No. CallId    dstCallId  LocalRTP   RmtRTP    LocalIP           RemoteIP         MPSS   VRF
1      1001      1002      25000     16400     10.0.0.1         10.0.0.2        NO     vrf1
2      1002      1001      29000     16392     11.0.0.1         11.0.0.2        NO     vrf2
```

```
Found 2 active RTP connections
```

In the above output, you can observe that for both the VRF's having non-overlapping rtp port ranges, the local RTP port allocated for vrf1 and vrf2 are different.

Example 2 - Overlapping Port Range

The following is example shows two VRFs with overlapping RTP port range:

```
Device(conf)# voice service voip
Device(conf-voi-serv)# no ip address trusted authenticate
Device(conf-voi-serv)# media bulk-stats
Device(conf-voi-serv)# media-address voice-vrf vrf1 port-range 25000 28000
Device(conf-voi-serv)# media-address voice-vrf vrf2 port-range 25000 28000
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# redundancy-group 1
Device(conf-voi-serv)# sip
```

The output for command **show voip rtp connections** shows as follows:

```
Device# show voip rtp connections

VoIP RTP Port Usage Information:
Max Ports Available: 23001, Ports Reserved: 101, Ports in Use: 2

          Min   Max   Ports   Ports
          -----
Ports
Media-Address Range      Port  Port  Available  Reserved  In-use
-----
Global Media Pool        8000  48198 19999      101       0
VRF ID Based Media Pool
-----
vrf1                      25000 28000 1501        0         1
vrf2                      25000 28000 1501        0         1
-----

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP  RmtRTP      LocalIP      RemoteIP      MPSS      VRF
-----
1      1001      1002      25000      16400      10.0.0.1      10.0.0.2      NO      vrf1
2      1002      1001      25000      16392      11.0.0.1      11.0.0.2      NO      vrf2

Found 2 active RTP connections
```

In the above output, you can observe that for both the VRF's having overlapping rtp port ranges, the local RTP port allocated for vrf1 and vrf2 is same.

Directory Number (DN) Overlap across Multiple-VRFs

CUBE has the capability to bridge calls across VRFs without the need for route leaks to be configured.

If multiple dial-peers on two different VRFs have the same destination-pattern and preference, CUBE will randomly choose a dial-peer and route the call using the session target of the selected dial-peer. Due to this, the call intended for one VRF may be routed to another VRF.

Dial-peer group feature allows you to route calls within the same VRF and not across VRFs. Configuring dial-peer group, routes the call to a specific VRF even if multiple dial-peers on two different VRFs have the same destination-pattern and preference.

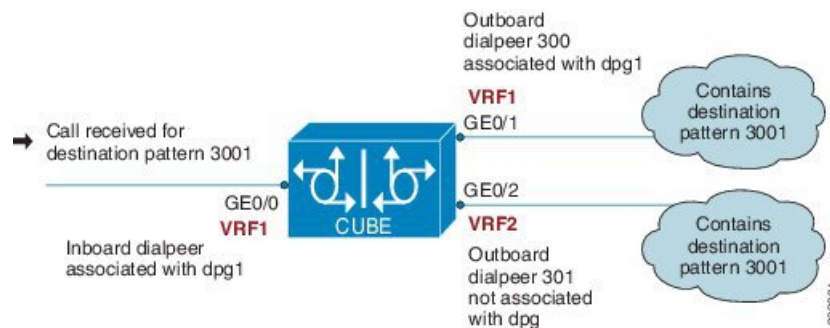
To use dial-peer group feature, configure dial-peers such that there is a unique inbound dial-peer match for calls related to each VRF. Configuring dial-peer group, limits the outbound dial-peer search within the VRF.

Example: Associating Dial-peer Groups to Overcome DN Overlap

If a call is received on VRF1 and there are two dial-peers with same destination-pattern (one dial-peer bind to VRF1 and second dial-peer bind to VRF2), then by default, CUBE picks the VRF in random to route the call.

If you intended to route this call only to VRF1 dial-peer, then dial-peer group can be applied on inbound dial-peer which will restrict the CUBE to route the call only across the dial-peers within the dial-peer group and not pick a dial-peer bind to a different VRF.

Figure 52: Associating Dial-peer Group to overcome DN overlap



The following scenario is considered in the below example:

- VRF1 associated with Gigabitethernt Interface 0/0 and 0/1
- VRF 2 associated with Gigabitethernet Inetrface 0/2
- Dial-peer Group: dpg1
- VRF1 is associated with dial-peer group - dpg 1
- Outbound dial-peer 300 is selected as preference 1
- Inbound dial-peer 3000 associated with VRF 1 and dial-peer group 1 (dpg1)
- Outbound Dial-peer: 300 – destination pattern “3001” associated with VRF1
- Outbound dial-peer: 301 – destination pattern “3001” associated with VRF2

Configure a dial-peer group and set the outbound dial-peer preference.

```
Device# enable
Device# configure terminal
Device(config)# voice class dpg 1
Device(voice-class)# dial-peer 300 preference 1
```

Create inbound dial-peer and associated with dial-peer group 1 (dpg1)

```
Device(config)# dial-peer voice 3000 voip
Device(config-dial-peer)# video codec h264
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session transport udp
```

```

Device(config-dial-peer)# destination dpg 1
Device(config-dial-peer)# incoming called-number 3001
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/1

Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/1
Device(config-dial-peer)# dtmf-relay sip-kpml
Device(config-dial-peer)# srtp fallback
Device(config-dial-peer)# codec g711ulaw

```

Creating outbound dial-peer with destination pattern ‘3001’ associated with VRF1.

```

Device(config)# dial-peer voice 300 voip
Device(config-dial-peer)# destination-pattern 3001
Device(config-dial-peer)# video codec h264
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.0.0.1
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/1
Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/1
Device(config-dial-peer)# dtmf-relay sip-kpml
Device(config-dial-peer)# codec g711ulaw

```

Creating outbound dial-peer with destination pattern ‘3001’ associated with VRF2.

```

Device(config)# dial-peer voice 301 voip
Device(config-dial-peer)# destination-pattern 3001
Device(config-dial-peer)# video codec h264
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:11.0.0.1
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/2
Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/2
Device(config-dial-peer)# dtmf-relay sip-kpml
Device(config-dial-peer)# codec g711ulaw

```

With above dial-peer group configuration, whenever dial-peer “3000” is matched as inbound dial-peer, CUBE will always route call using dial-peer “300” (VRF1). Without dial-peer group, CUBE would have picked dial-peers “300”(VRF1) and “301”(VRF2) in random to route the call.

```
Device# show vrf brief
```

Name	Default RD	Protocols	Interfaces
VRF1	1:1	ipv4	Gi0/0 Gi0/1
VRF2	2:2	ipv4	Gi0/2

```
Device# show dial-peer voice summary
```

```
dial-peer hunt 0
```

TAG	TYPE	MIN	AD	OPER	PREFIX	DEST-PATTERN	PRE	PASS	SESS-TARGET	OUT	
KEEPALIVE		VRF					FER	THRU		STAT	PORT
3000	voip	up	up				0	syst			
300	voip	up	up		3001		0	syst	ipv4: 10.0.0.1		
301	voip	up			3001		0	syst	ipv4: 11.0.0.1		

IP Overlap with VRF

Generally, on a router, two interfaces cannot be configured with the same IP address. With the VRF feature, you can configure two or more interfaces with the same IP address because, each interface having the same

IP address belongs to a unique VRF and hence belongs to a different routing domain. However, for successful call processing, you must ensure that appropriate call routing protocols are configured on the VRFs.

The following is a sample configuration:

Configure Gigabit Ethernet 0/0 that belongs to VRF1 with IP address 10.0.0.0.

```
Device# enable
Device# configure terminal
Device(config)# ip vrf VRF1
Device(config)# rd 1:1
Device(config)# exit

Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0
Device(config-if)# ip vrf forwarding VRF1
Device(config-if)# ip address 10.0.0.0 255.255.255.0
Device(config-if)# speed auto
Device(config-if)# exit
```

Configure Gigabit Ethernet 0/1 that belongs to VRF2 with IP address 10.0.0.0.

```
Device# enable
Device# configure terminal
Device(config)# ip vrf VRF2
Device(config)# rd 1:1
Device(config)# exit

Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/1
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.0 255.255.255.0
Device(config-if)# speed auto
Device(config-if)# exit
```

For call routing on VRF1 and VRF2, ensure that appropriate routing entries are configured for both VRF1 and VRF2.



Note The above configurations are specific to VRF support only. For call routing, appropriate routing protocols must be configured in the network.

Even though Gigabit Ethernet 0/0 and Gigabit Ethernet 0/1 have an overlapping IP address, the call processing is not overlapped as they belong to different VRFs.

show ip interface brief command shows that GigabitEthernet 0/0 and GigabitEthernet 0/1 have an overlapping IP address:

```
Device# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0  8.44.22.2      YES NVRAM  up          up
GigabitEthernet0/0/1  unassigned     YES NVRAM  administratively down down
Service-Engine0/1/0  unassigned     YES unset  up          up
Service-Engine0/2/0  unassigned     YES unset  up          up
GigabitEthernet0     unassigned     YES NVRAM  administratively down down
```

show voip rtp connections command shows a video call that is established on CUBE across different interfaces belonging to different VRFs having Overlap IP address:

```
Device# show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 11700, Ports Reserved: 303, Ports in Use: 4
```

Media-Address Range	Min Port	Max Port	Ports Available	Ports Reserved	Ports In-use
Global Media Pool	20000	22000	900	101	0
VRF ID Based Media Pool					
POD2	30002	32000	1000	0	0
POD1	20000	30000	4900	101	2
POD3	20000	30000	4900	101	2

```
VoIP RTP active connections :
No. CallId      dstCallId  LocalRTP  RmtRTP   LocalIP   RemoteIP  MPSS  VRF
1      37         39        20000    18164    10.0.0.0  11.0.0.3  NO   VRF1
2      38         40        20002    18166    10.0.0.0  11.0.0.3  NO   VRF1
3      39         37        20002    16388    10.0.0.0  11.0.0.3  NO   VRF2
4      40         38        20000    16390    10.0.0.0  11.0.0.3  NO   VRF2
Found 4 active RTP connections
```

Use Server Groups with VRF

Whenever destination server group is used with VRF, ensure that the server group should have the session targets, belonging to the same network as that of sip bind on the dial-peer, where the server-group is configured. This is because the dial-peer bind is mandatory with VRF and only one sip bind can be configured on any given dial-peer.

The following scenario is considered in the below example:

Interfaces and associated IP address

- GigabitEthernet0/0/2 12.0.0.1
- GigabitEthernet0/0/1 11.0.0.1

```
Device# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	10.0.0.1	YES	NVRAM	up	up
GigabitEthernet0/0/1	11.0.0.1	YES	NVRAM	up	up
GigabitEthernet0/0/2	12.0.0.1	YES	NVRAM	up	up

- dial-peer 200 is bind to GigabitEthernet0/0/1
- server-group 1 (belonging to VRF1) is applied to dial-peer 200

```
Device(config)# dial-peer voice 200 voip
Device(config-dialpeer)# destination-pattern 4.....
Device(config-dialpeer)# session protocol sipv2
Device(config-dialpeer)# session transport udp
Device(config-dialpeer)# session server-group 1
Device(config-dialpeer)# voice-class sip bind control source-interface GigabitEthernet0/0/1
Device(config-dialpeer)# voice-class sip bind media source-interface GigabitEthernet0/0/1
```

```
Device(config-dialpeer)# codec g711ulaw
```

As dial-peer 200 is bind to GigabitEthernet0/0/1 , the session targets configured in the “server-group 1” should belong to the network which is reachable by the bind source interface GigabitEthernet0/0/1 as shown below:

```
Device(config)# voice class server-group 1
Device(config-class)# ipv4 11.0.0.22
Device(config-class)# ipv4 11.0.0.8 preference 2
```

Inbound Dial-Peer Matching Based on Multi-VRF

From Cisco IOS Release 15.6(3)M and Cisco IOS XE Denali 16.3.1 onwards, dial-peer matching is done based on the VRF ID associated with a particular interface.

Example: Inbound Dial-Peer Matching based on Multi-VRF

Prior to Cisco IOS 15.6(3)M and Cisco IOS XE Denali 16.3.1 releases, when an incoming out-of-dialog message such as INVITE, REGISTER, OPTIONS, NOTIFY, and so on are received on a particular VRF bound interface, inbound dial-peer matching was done using the complete set of inbound dial-peers regardless of the VRF association. The response would be sent based on this matched dial-peer. Since the inbound dial-peer selected could have a different VRF bound to it, the response was sent to the wrong VRF.

To overcome this issue, the inbound dial-peers are filtered based on the incoming VRF and then followed by the regular inbound dial-peer matching. Now, the response is sent to the same VRF on which the request was received.

Consider the following configuration example output to understand the inbound dial-peer matching criteria used in multi-VRF:

```
interface GigabitEthernet0/0/0
ip address 8.39.18.37 255.255.0.0
duplex auto
ip vrf forwarding VRF ID1
speed auto

interface GigabitEthernet0/0/1
ip address 9.39.18.55 255.255.0.0
duplex auto
ip vrf forwarding VRF ID2
speed auto

interface GigabitEthernet0/0/2
ip address 10.39.18.68 255.255.0.0
duplex auto
ip vrf forwarding VRF ID3
speed auto

dial-peer voice 1000 voip
description "Inbound dial-peer bound to VRF ID2"
session protocol sipv2
session target sip-server
session transport udp
incoming called-number 5678
voice-class sip bind control source-interface GigabitEthernet0/0/1
voice-class sip bind media source-interface GigabitEthernet0/0/1
```



```
codec g711ulaw

dial-peer voice 2000 voip
description "Inbound dial-peer bound to VRF ID1"
session protocol sipv2
session target sip-server
session transport udp
incoming called-number 5678
voice-class sip bind control source-interface GigabitEthernet0/0/0
voice-class sip bind media source-interface GigabitEthernet0/0/0
codec g711ulaw

dial-peer voice 3000 voip
description "Inbound dial-peer bound to VRF ID3"
session protocol sipv2
session target sip-server
session transport udp
incoming called-number 8000
voice-class sip bind control source-interface GigabitEthernet0/0/2
voice-class sip bind media source-interface GigabitEthernet0/0/2
codec g711ulaw

dial-peer voice 4000 voip
description "Inbound dial-peer bound to VRF ID1"
session protocol sipv2
session target sip-server
session transport udp
incoming called-number 2000
voice-class sip bind control source-interface GigabitEthernet0/0/0
voice-class sip bind media source-interface GigabitEthernet0/0/0
codec g711ulaw
```

With the introduction of VRF aware inbound dial-peer matching, the initial filtering is done based on the VRF ID and then based on the called-number. For the above example, a call with called-number of 5678 that is received on GigabitEthernet 0/0 with VRF ID 1 configured, the dial-peers will first be filtered to those that are bound to GigabitEthernet 0/0 before selection of the inbound dial-peer is performed. Now, the response is sent successfully on VRF ID1.



Note Whenever the VRF ID is added, modified, or removed under the interface, it is mandatory to execute the following command before making any calls: **clear interface** <interface>. If the **clear interface** <interface> command is not executed, the dial-peer is bound to the old VRF ID and not to the new VRF ID.



Note Inbound dial-peer matching based on VRF ID is selected in the following order of preference:

1. Dial-peer based configuration
 2. Tenant based configuration
 3. Global based configuration
-

Example: Tenant based Inbound Dial-Peer Matching

```
voice class tenant 1
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
  dial-peer voice 2000 voip
    description "Inbound dial-peer bound to VRF-ID 1"
    session protocol sipv2
    session target sip-server
    session transport udp
    incoming called-number 5678
  voice-class sip tenant 1
  codec g711ulaw
```

Example: Global based Inbound Dial-Peer Matching

```
voice service voip
  sip
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
```

VRF Aware DNS for SIP Calls

The VRF Aware DNS for SIP Calls feature enables you to specify the Virtual Routing and Forwarding (VRF) table so that the domain name system (DNS) can forward queries to name servers using the VRF table.

Because the same IP address can be associated with different DNS servers in different VRF domains, a separate list of name caches for each VRF is maintained. The DNS looks up the specific VRF name cache before sending a query to the VRF name server. All IP addresses obtained from a VRF-specific name cache are routed using the VRF table.

While processing a SIP call, if a hostname has to be resolved, only the VRF associated with the SIP call is used during DNS resolutions.



Note Ensure that the name-server is configured using **ip name-server vrf** command. For configuration details, see [Name Server Configuration](#).

High Availability with VRF

CUBE supports VRF in RG Infra high availability mode. VRF is supported on CUBE box-to-box and inbox high availability types.

For box-to-box high availability in Aggregation Services Routers 1000 Series and Integrated Services Routers 4000 Series, RG interface must not be associated with VRF where as the inbound and outbound interfaces (meant for handling VoIP traffic) can be associated with VRF's depending upon the deployment.

All the configurations including the VRF based RTP port range has to be identical on active and standby routers. VRF IDs will be check pointed before and after the switchover.

Configuration Examples

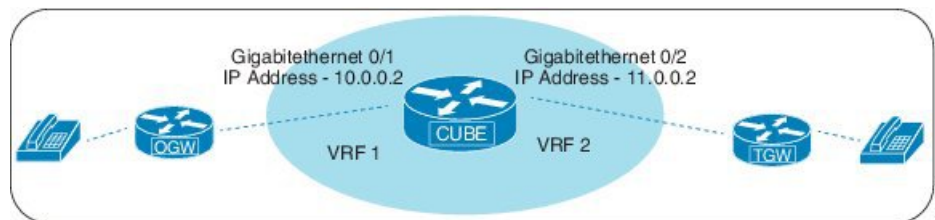


Note The steps in the following configuration example is for a new network and hence it is assumed that there is no existing configuration.

Example: Configuring Multi-VRF in Standalone Mode

The configuration in this scenario is as shown below where the GigabitEthernet 0/1 is assigned to VRF1 and GigabitEthernet 0/2 is assigned to VRF2.

Figure 53: Multi-VRF in Standalone Mode



Configuring VRF

```
Device# enable
Device# configure terminal
Device(config)# ip vrf VRF1
Device(config)# rd 1:1
Device(config)# ip vrf VRF2
Device(config)# rd 2:2
Device(config)# exit
```

Associating interfaces with VRF

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip vrf forwarding VRF1
Device(config)# interface GigabitEthernet0/2
Device(config-if)# ip vrf forwarding VRF2
```



Note If an IP address is already assigned to an interface, then associating a VRF with interface will disable the interface and remove the existing IP address. An error message (sample error message shown below) is displayed on the console. Assign the IP address to proceed further.

```
% Interface GigabitEthernet0/1 IPv4 disabled and address(es) removed due to
enabling VRF VRF1
```

Configure Interface GigabitEthernet0/1

```

Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip address 10.0.0.2 255.255.255.0
Device(config-if)# speed auto
Device(config-if)# exit

```

Configure Interface GigabitEthernet0/2

```

Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip address 11.0.0.2 255.255.255.0
Device(config-if)# speed auto
Device(config-if)# exit

```

Creating Dial-peer

Creating Inbound Dial-peer:

```

Device(config)# dial-peer voice 1111 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# incoming called-number 1111
Device(cofig-dial-peer)# codec g711ulaw

```

Creating Outbound Dial-peer:

```

Device(config)# dial-peer voice 2222 voip
Device(config-dial-peer)# destination pattern 1111
Device(config-dial-peer)# session protocol sipv2

```

Execute the following command to verify the dial-peer association with interface:

```

Device# show dial-peer voice summary

```

TAG	TYPE	MIN	OPER	PREFIX	DEST-PATTERN	PRE	PASS	SESS-TARGET	STAT	PORT	KEEPALIVE	VRF
1111	voip	up	up		-	0	syst	ipv4:10.0.0.2				
VRF1												
2222	voip	up	up		-	0	syst	ipv4:11.0.0.2				
VRF2												

Configure Binding

**Note**

- Control and Media on a dial-peer have to bind with same VRF. Else, while configuring, the CLI parser will display an error.
- Whenever global sip bind interface associated with a VRF is added, modified, or removed, you should restart the sip services under voice service voip sip mode so that the change in global sip bind comes into effect with associated VRF ID.

```
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# call service stop
Device(conf-serv-sip)# no call service stop
Device(conf-serv-sip)# end
```

```
Device(config)# dial-peer voice 1111 voip
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/0/1
Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/1
```

```
Device(config)# dial-peer voice 2222 voip
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/0/2
Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/0/2
```

Execute the following command to verify the interface association with VRF:

```
Device# show ip vrf brief
```

Name	Default RD	Interfaces
Mgmt-intf	<not set>	Gi0

Execute the following command to verify a successful and active calls:

For a single call, you should be able to see two RTP connections as shown in the below example.

```
Device# show voip rtp connections
```

```
VoIP RTP Port Usage Information:
Max Ports Available: 23001, Ports Reserved: 101, Ports in Use: 2
```

Media-Address Range	Min Port	Max Port	Ports Available	Ports Reserved	Ports In-use
Global Media Pool	8000	48198	19999	101	0

```
VoIP RTP active connections :
```

No.	CallId	dstCallId	LocalRTP	RmtRTP	LocalIP	RemoteIP	MPSS	VRF
1	1	2	25000	16390	10.0.0.1	10.0.0.2	NO	VRF1
2	2	1	25002	16398	11.0.0.1	11.0.0.2	NO	VRF2

```
Device# show call active voice brief -
```

```
Perf-AR1006#show call active voice brief
<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation>
```

Example: Configuring Multi-VRF in Standalone Mode

```

media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded>

media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
LostPacketRate:<%> OutOfOrderRate:<%>
VRF:<%>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
  last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l>
dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
  speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
  rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
11FF : 8565722 511605450ms.1 (*16:21:53.676 IST Tue Aug 4 2015) +30 pid:400001
Answer 777412373 active
  dur 00:00:22 tx:1110/66600 rx:1111/66660 dscp:0 media:0 audio tos:0xB8 video tos:0x0
  IP 10.0.0.2:30804 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay:
off Transcoded: No ICE: Off
  media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
  long duration call detected:n long duration call duration:n/a timestamp:n/a
  LostPacketRate:0.00 OutOfOrderRate:0.00
  VRF: VRF1
11FF : 8565723 511605470ms.1 (*16:21:53.696 IST Tue Aug 4 2015) +0 pid:400000 Originate
777512373 active
  dur 00:00:22 tx:1111/66660 rx:1110/66600 dscp:0 media:0 audio tos:0xB8 video tos:0x0
  IP 11.0.0.2:30804 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay:
off Transcoded: No ICE: Off
  media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
  long duration call detected:n long duration call duration:n/a timestamp:n/a
  LostPacketRate:0.00 OutOfOrderRate:0.00
  VRF: VRF2

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

Device# show sip-ua connections udp brief

Total active connections      : 2
No. of send failures          : 0
No. of remote closures       : 0

```

```
No. of conn. failures      : 0
No. of inactive conn. ageouts : 2
```

```
----- SIP Transport Layer Listen Sockets -----
Conn-Id      Local-Address
=====
2             [10.0.0.1]:5060:VRF1
3             [11.0.0.1]:5060:VRF2
```

Device# **show call active voice compact**

```
<callID>  A/O  FAX T<sec>  Codec      type  Peer Address  IP R<ip>:<udp>  VRF
Total call-legs: 2
8565722  ANS   T12   g711ulaw  VOIP  P777412373  10.0.0.2:30804  VRF1
8565723  ORG   T12   g711ulaw  VOIP  P777512373  11.0.0.2:30804  VRF2
```

Device# **show call active video compact**

```
MVRF-CUBE1#show call active video compact
<callID>  A/O  FAX T<sec>  Codec type      Peer Address  IP R<ip>:<udp>  VRF
Total call-legs: 2
10193983  ANS   T30   H264  VOIP-VIDEO  P2005         10.0.0.2:18078  VRF1
10193985  ORG   T30   H264  VOIP-VIDEO  P3001         11.0.0.2:27042  VRF2
```

Example: Configuring RG Infra High Availability with VRF

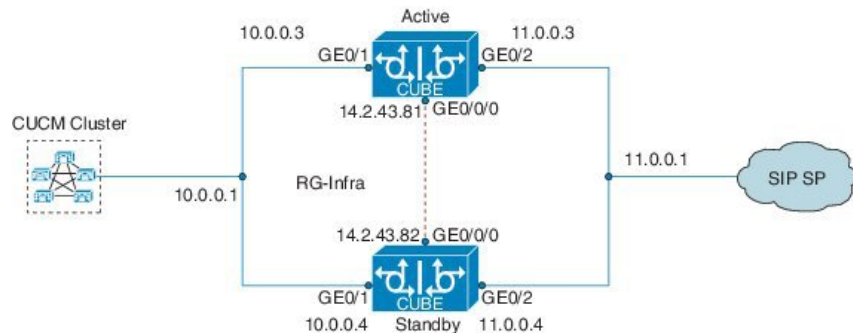


Note Below configuration example is applicable for Cisco ASR 1000 Series Aggregated Services Routers (ASR) and Cisco 4000 Series Integrated Services Routers (ISR G3).



Note Do not configure VRF on the interface that is used for RG Infra. Traffic of VRF and RG Infra should be on different interfaces.

Figure 54: Multi-VRF in High Availability Mode (RG Infra)



Configuration on Active Router



Note The configurations of Active Router and Stand By Router should be identical.

Configuring VRF

```
Device> enable
Device# configure terminal
Device(config)# ip vrf VRF1
Device(config)# rd 1:1
Device(config)# ip vrf VRF2
Device(config)# rd 2:2

Device(config)# voice service voip
Device(config)# no ip address trusted authenticate
Device(config)# media bulk-stats
Device(config)# allow-connections sip to sip
Device(config)# redundancy-group 1
Device(config)# sip

Device(config)# redundancy
Device(config)# mode none
Device(config)# application redundancy
Device(config)# group 1
Device(config)# name raf-b2b
Device(config)# priority 1
Device(config)# timers delay 30 reload 60
Device(config)# control GigabitEthernet0/0/0 protocol 1
Device(config)# data GigabitEthernet0/0/0
```

Associating interfaces with VRF

```
Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip vrf forwarding vrf2
```



Note If an IP address is already assigned to an interface, then associating a VRF with interface will disable the interface and remove the existing IP address. An error message (sample error message shown below) is displayed on the console. Assign the IP address to proceed further.

```
% Interface GigabitEthernet0/0/1 IPv4 disabled and address(es) removed due to
enabling VRF VRF1
```

GigabitEthernet0/0/0 is used for configuring RG Infra and therefore do not configure any VRF with this interface.

```
Device(config)# interface GigabitEthernet0/0/0
Device(config-if)# ip address 14.2.43.81 255.255.0.0
Device(config-if)# negotiation auto
Device(config-if)# cdp enable
```

Inbound interface - GigabitEthernet0/0/1 is used for voice traffic configured with VRF1.


```

Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip vrf forwarding VRF1
Device(config-if)# ip address 10.0.0.3 255.0.0.0
Device(config-if)# negotiation auto
Device(config-if)# cdp enable
Device(config-if)# redundancy rii 1
Device(config-if)# redundancy group 1 ip 10.0.0.1 exclusive

```

Outbound interface - GigabitEthernet0/2 is used for voice traffic configured with VRF2.

```

Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 11.0.0.3 255.0.0.0
Device(config-if)# negotiation auto
Device(config-if)# cdp enable
Device(config-if)# redundancy rii 2
Device(config-if)# redundancy group 1 ip 11.0.0.1 exclusive

```

Creating Dial-peer

Creating Inbound Dial-peer:

```

Device(config)# dial-peer voice 1111 voip
Device(config-dial-peer)# destination pattern 1111
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.0.0.2
Device(config-dial-peer)# incoming called-number 1111

```

Creating Outbound Dial-peer:

```

Device(config)# dial-peer voice 3333 voip
Device(config)# destination-pattern 2222
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:11.0.0.2

```

Configuring Binding



Note Control and Media on a dial-peer have to bind with same VRF. Else, while configuring, the CLI parser will display an error.

```

Device(config)# dial-peer voice 1111 voip
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/0/1
Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/0/1

Device(config)# dial-peer voice 3333 voip
Device(config-dial-peer)# voice-class sip bind control source-interface GigabitEthernet0/0/2
Device(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet0/0/2

```

Configuration on Standby Router



Note The configurations of Active and Stand By should be identical.

Configuring VRF

```
Device> enable
Device# configure terminal
Device(config)# ip vrf VRF1
Device(config)# rd 1:1
Device(config)# ip vrf VRF2
Device(config)# rd 2:2

Device(config)# voice service voip
Device(config)# no ip address trusted authenticate
Device(config)# media bulk-stats
Device(config)# allow-connections sip to sip
Device(config)# redundancy-group 1
Device(config)# sip

Device(config)# redundancy
Device(config)# mode none
Device(config)# application redundancy
Device(config)# group 1
Device(config)# name raf-b2b
Device(config)# priority 1
Device(config)# timers delay 30 reload 60
Device(config)# control GigabitEthernet0/0/0 protocol 1
Device(config)# data GigabitEthernet0/0/0
```

Associating interfaces with VRF

```
Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip vrf forwarding VRF2
```



Note If an IP address is already assigned to an interface, then associating a VRF with interface will disable the interface and remove the existing IP address. An error message (sample error message shown below) is displayed on the console. Assign the IP address to proceed further.

```
% Interface GigabitEthernet0/0/1 IPv4 disabled and address(es) removed due to
enabling VRF VRF1
```

GigabitEthernet0/0/0 is used for configuring RG Infra and therefore do not configure any VRF with this interface.

```
Device(config)# interface GigabitEthernet0/0/0
Device(config-if)# ip address 14.2.43.81 255.255.0.0
Device(config-if)# negotiation auto
Device(config-if)# cdp enable
```

Inbound interface - GigabitEthernet0/0/1 is used for voice traffic configured with VRF1.

```

Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip vrf forwarding VRF1
Device(config-if)# ip address 10.0.0.4 255.0.0.0
Device(config-if)# negotiation auto
Device(config-if)# cdp enable
Device(config-if)# redundancy rii 1
Device(config-if)# redundancy group 1 ip 10.0.0.1 exclusive

```

Outbound interface - GigabitEthernet0/0/2 is used for voice traffic configured with VRF2.

```

Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 11.0.0.4 255.0.0.0
Device(config-if)# negotiation auto
Device(config-if)# cdp enable
Device(config-if)# redundancy rii 2
Device(config-if)# redundancy group 1 ip 11.0.0.1 exclusive

```

Creating Dial-peer

Creating Inbound Dial-peer:

```

Device(config)# dial-peer voice 1111 voip
Device(config-dial-peer)# destination pattern 1111
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.0.0.2
Device(config-dial-peer)# incoming called-number 1111

```

Creating Outbound Dial-peer:

```

Device(config)# dial-peer voice 3333 voip
Device(config)# destination-pattern 2222
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:11.0.0.2

```

Configuring Binding



Note Control and Media on a dial-peer have to bind with same VRF. Else, while configuring, the CLI parser will display an error.

```

Device(config)# dial-peer voice 1111 voip
Device(config-dial-peer)# voice-class sip bind control source-interface
GigabitEthernet0/1
Device(config)# voice-class sip bind media source-interface
GigabitEthernet0/1

Device(config)# dial-peer voice 3333 voip
Device(config)# voice-class sip bind control source-interface GigabitEthernet0/0/2
Device(config)# voice-class sip bind media source-interface GigabitEthernet0/0/2

```

Verification of Calls Before and After Switchover

RTP Connections on Active router:

```
Device# show voip rtp connections
```

```
VoIP RTP Port Usage Information:
```

```
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 2
```

Media-Address Range	Min Port	Max Port	Ports Available	Ports Reserved	Ports In-use
Global Media Pool	8000	48198	19999	101	2

```
VoIP RTP active connections :
```

No.	CallId	dstCallId	LocalRTP	RmtRTP	LocalIP	RemoteIP	MPSS	VRF
1	5	6	8008	16388	10.0.0.1	10.0.0.2	NO	VRF1
2	6	5	8010	16388	11.0.0.1	11.0.0.2	NO	VRF2

Found 2 active RTP connections

RTP Connections on Standby Router after switchover

```
Device# show voip rtp connections
```

```
VoIP RTP Port Usage Information:
```

```
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 2
```

Media-Address Range	Min Port	Max Port	Ports Available	Ports Reserved	Ports In-use
Global Media Pool	8000	48198	19999	101	2

```
VoIP RTP active connections :
```

No.	CallId	dstCallId	LocalRTP	RmtRTP	LocalIP	RemoteIP	MPSS	VRF
1	7	8	8012	16390	10.0.0.1	10.0.0.2	NO	VRF1
2	8	7	8014	16390	11.0.0.1	11.0.0.2	NO	VRF2

```
Found 2 active RTP connections
```

Active calls on Active Router

```
Device# show call active voice brief
```

```
11F3 : 5 243854170ms.1 (*11:48:43.972 UTC Mon May 25 2015) +6770 pid:0 Answer active
dur 00:00:14 tx:843/50551 rx:1028/61680 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.0.0.2:16388 SRTP: off rtt:lms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay:
off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```
11F3 : 6 243854170ms.2 (*11:48:43.972 UTC Mon May 25 2015) +6770 pid:3333 Originate 2222
active
dur 00:00:14 tx:1028/61680 rx:843/50551 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 11.0.0.2:16388 SRTP: off rtt:65522ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay:
off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

```

```
Device#show sip-ua connections udp brief
```

```

Total active connections      : 2
No. of send failures         : 0
No. of remote closures       : 0
No. of conn. failures        : 0
No. of inactive conn. ageouts : 2

```

```

----- SIP Transport Layer Listen Sockets -----
Conn-Id      Local-Address
=====
2            [10.0.0.1]:5060:VRF1
3            [11.0.0.1]:5060:VRF2

```

Active calls on Standby router after switchover:

```
Device# show call active voice brief
```

```

11F9 : 8 245073830ms.1 (*12:16:18.094 UTC Mon May 25 2015) +26860 pid:3333 Originate 2222
connected
dur 00:03:37 tx:6757/405420 rx:6757/405420 dscp:0 media:0 audio tos:0x0 video tos:0x0
IP 11.0.0.2:16390 SRTP: off rtt:65531ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay:
off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

```

```

11F9 : 7 245073850ms.1 (*12:16:18.114 UTC Mon May 25 2015) +26840 pid:0 Answer connected
dur 00:03:37 tx:6757/405420 rx:6757/405420 dscp:0 media:0 audio tos:0x0 video tos:0x0
IP 10.0.0.2:16390 SRTP: off rtt:65523ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8 TextRelay:
off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

```

```

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

```

Troubleshooting Tips

The following commands are helpful for troubleshooting:

- **show voip rtp connections**

The following is an example where media flow-around is configured. The output shows 0 connections since media does not flow through CUBE.

```
Device#show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 19999, Ports Reserved: 101, Ports in Use: 0
Port range not configured
```

Media-Address Range	Min Port	Max Port	Ports Available	Ports Reserved	Ports In-use
Global Media Pool	8000	48198	19999	101	0

```
No active connections found
```

- **show call active voice compact**

```
Device#show call active voice compact
<callID> A/O FAX T<sec> Codec type Peer Address IP R<ip>:<udp> VRF
4021 ORG T45 g711ulaw VOIP P7474 8.41.17.71:27754 VRF1
4020 ANS T45 g711ulaw VOIP Psipp 8.41.17.71:17001 VRF1
```

- **debug ccsip verbose**

The output of **debug ccsip verbose** command is wordy and may cause issues when enabled on a busy network environment.



PART **XI**

High Availability

- [High Availability on Cisco 4000 Integrated Services Routers and Cisco Catalyst 8000 Series Edge Platforms, on page 735](#)
- [High Availability on Cisco ASR 1000 and Cisco Catalyst 8000 Series Routers, on page 757](#)
- [High Availability on Cisco C8000V Series Cloud Services Routers, on page 787](#)
- [DSP High Availability Support, on page 803](#)
- [Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices, on page 807](#)
- [CVP Survivability TCL support with High Availability, on page 821](#)



CHAPTER 66

High Availability on Cisco 4000 Integrated Services Routers and Cisco Catalyst 8000 Series Edge Platforms

- [Overview, on page 735](#)
- [Considerations and Restrictions, on page 739](#)
- [Configure CUBE High Availability on Cisco 4000 Series ISR and Cisco Catalyst 8000 Series Edge Platforms, on page 741](#)
- [Verify Your Configuration, on page 748](#)
- [Tips to Troubleshoot, on page 755](#)

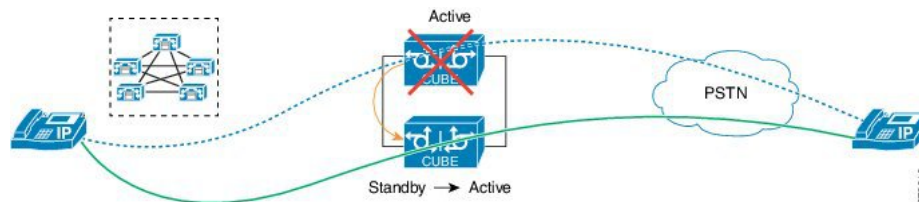
Overview



Note The H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

The High Availability (HA) feature allows you to benefit from the failover capability of Cisco Unified Border Element (CUBE) on two routers, one active and one standby. When the active router goes down for any reason, the standby router takes over seamlessly, preserving and processing your calls.

Figure 55: CUBE High Availability



CUBE supports Box-to-box redundancy on Cisco 4000 Series Integrated Services Router (Cisco 4000 Series ISR), Cisco Catalyst 8300, 8200, and 8200-L Series Edge Platforms and uses Redundancy Group Infrastructure to provide High Availability.

Feature Information

Table 92: Feature Information

Feature Name	Releases	Feature Information
High Availability Support on Cisco Unified Border Element (CUBE)	Baseline Functionality	CUBE supports redundancy and failover capability on active and standby routers.
IPv6 flows in High Availability	Cisco IOS XE Dublin 17.12.1a	The support for IPv6 flows in high availability is introduced.

Box-to-Box Redundancy

Box-to-box redundancy enables configuring a pair of routers to act as back up for each other. In the router pair, the active router is determined based on the failover conditions. The router pair continuously exchange status messages. CUBE session information is checkpointed across the active and standby router. This enables the standby router to immediately take over all CUBE call processing responsibilities when the active router becomes unavailable.

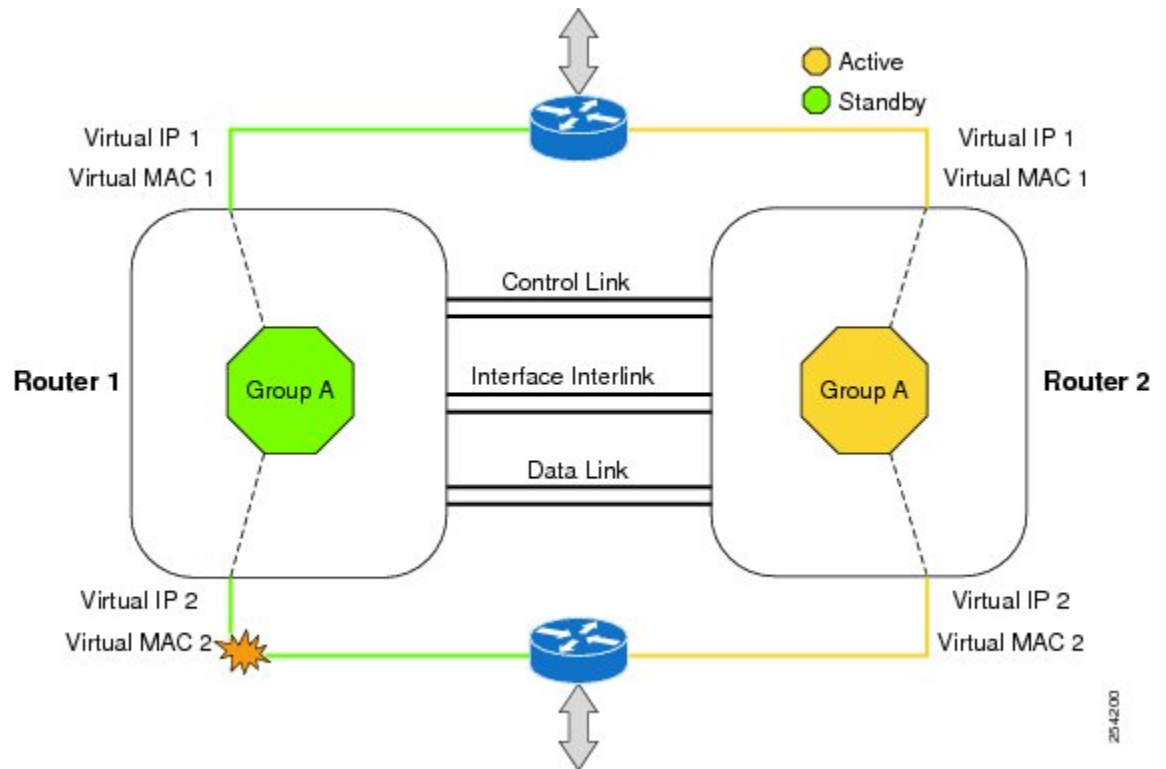
Redundancy Group (RG) Infrastructure

A group of redundant interfaces form a Redundancy Group. The active and standby routers are connected by a configurable control link and data synchronization link. The control link is used to communicate the redundancy state for each router. The data synchronization link is used to transfer stateful information to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces is configured with the same unique ID number, also known as the Redundancy Interface Identifier (RII).

A Virtual IP address (VIP) is configured on interfaces that connect to the external network. All signaling and media is sourced from and sent to the Virtual IP address. External devices such as Cisco Unified Communication Manager, uses VIP as the destination IP address for the calls traversing through CUBE.

The following figure shows the redundancy group configured for a pair of routers with a single outgoing interface.

Figure 56: Redundancy Group Configuration



Network Topology

This section describes how to configure the following network topology, in which an active and standby pair of routers is used in a SIP trunk deployment between a Cisco Unified Communications Manager (Unified CM) and a service provider (SP) SIP trunk for PSTN access.

In this topology, both active and standby routers have the same configuration and both platforms are connected through a physical switch across same interfaces. This is required for CUBE HA to work. For example, the CUBE-1 and CUBE-2 interface towards WAN must terminate on the same switch. Multiple interfaces or sub-interfaces can be used on either LAN or WAN side. Also, one CUBE has a lower IP address across all three interfaces on the same CUBE platform.

We recommend that you keep the following in mind when configuring this topology:

- Connect the redundancy group control and data interfaces in the CUBE HA pair to the same physical switch to avoid any latency in the network.
- The RG control and data interfaces of the CUBE HA pair can be connected through a back-to-back cable or using a switch as shown in the following figures:

Figure 57: Network Topology with switch between active and standby routers

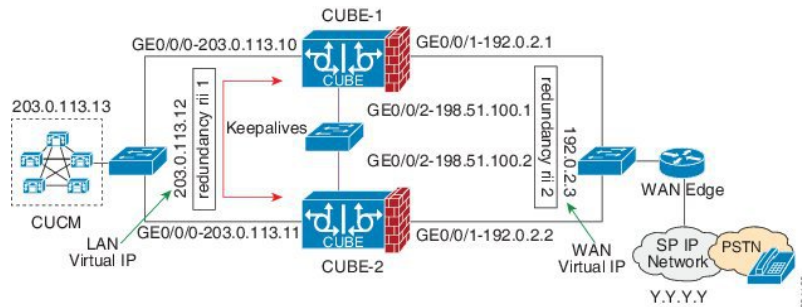
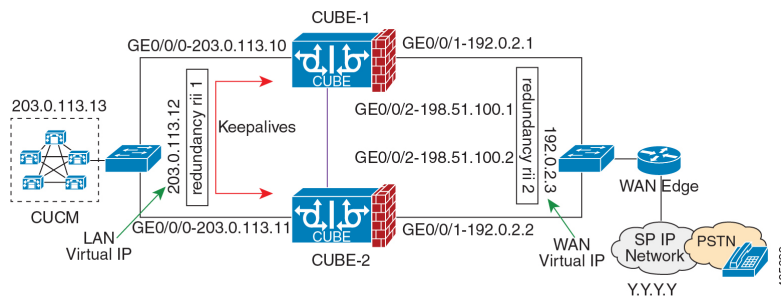


Figure 58: Network Topology with crossover cable between active and standby routers



Note However, it is recommended to use Portchannel for the RG control and data interfaces for redundancy. A single connection using back-to-back cable or switch presents a single point of failure due to a faulty cable, port, or switch, resulting in error state where both routers are Active.

- If the RG ID is the same for the two different CUBE HA pairs, keepalive interface for check-pointing the RG control and data, and traffic must be in a different subnet or VLAN.



Note This recommendation is applicable only if you connect using a switch, not by back-to-back cables.

- You can configure a maximum of two redundancy groups. Hence, there can be only two Active and Standby pairs within the same network.



Note This recommendation is applicable only if you connect using a switch, not by back-to-back cables.

- Source all signaling and media from and to the Virtual IP address.
- Always save the running configuration to avoid losing it due to router reload during a failover.

- Virtual Routing and Forwarding
 - Define Virtual Router Forwarding (VRF) in the same order on both active and standby routers for an accurate synchronization of data.
 - You can configure VRFs only on Traffic interfaces (SIP and RTP). Do not configure VRF on RG Control and Data interface.
 - VRF configurations on both the active and standby router must be identical. VRF IDs are checkpointed for the calls before and after switchover (includes VRF-based RTP port range).
- Manually copy the configurations from one router to the other.
- Replicating the configuration on the Standby router does not commit to the startup configuration; it is in the running configuration. You must run the **write memory** command to commit the changes that are synchronized from the active router on the standby router.

Considerations and Restrictions

The following is a list of further considerations and restrictions you should know before configuring this topology:

Considerations

- The same platform and configurations including interface must be used for the Active and Standby routers.
- IPv6 flows in high availability is supported starting from Cisco IOS XE Dublin 17.12.1a release.
- Only active calls are checkpointed (Calls that are connected with 200 OK or ACK transaction completed).
- When you apply and save the configuration for the first time, the platform must be reloaded.
- If you have Cisco Unified Customer Voice Portal (CVP) in your network, we recommend that you configure TCP session transport for the SIP trunk between CVP and CUBE.
- Upon failover, the previously active CUBE reloads by design.
- Smart Licensing communications happen through an active CUBE.
- Transport layer sessions (TCP/TLS/UDP) are not check-pointed between high availability pair and check will not be preserved.
- TCP sessions are not preserved during the failover. Remote user agents are expected to reestablish TCP sessions (using port 5060 or 5061) before sending subsequent messages.
- Call Admission Control (CAC) state is maintained through switchover. After Stateful Switchover, no calls are allowed if the CAC limit is reached before the switchover.
- Up to six multimedia lines in the SDP are checkpointed for CUBE high availability. From Cisco IOS XE Release 3.17 onwards, SDP Passthru (up to two m-lines) calls are also checkpointed.
- Survivability.tcl preservation is supported from Cisco IOS XE Release 3.17 onwards for Unified Customer Voice Portal (CVP) deployments.

- Out-of-band DTMF (Notify or KPML) is not supported post switchover. Only rtp-nte to rtp-nte and voice-inband to voice-inband DTMF works after the switchover.
- Media-flow around and UC Services API (Cisco Unified Communications Manager Network-Based Recording) are not supported.
- You cannot terminate Wide Area Network (WAN) on CUBE directly or Data HA on either side. Both active and standby routers must be in the same Data Center and connected to the same physical switch.
- The Courtesy Callback (CCB) feature is not supported if a callback was registered with Cisco Unified Customer Voice Portal (CVP) and then a switchover was done on CUBE.
- You cannot configure a secondary IP address for the interfaces.
- If the redundancy group ID is same for the two different CUBE HA pairs, then the keepalive interface that is used for checkpointing RG control and data traffic must be in a different subnet or VLAN.
- Call Progress Analysis (CPA) calls (before transferred to the agent), SCCP-based media resources, Noise Reduction, Acoustic Shock Protection (ASP), and transrating calls are not supported.
- Transport layer sessions tcp/tls/udp are not preserved or checkpointed to standby.
- The failover time for a Box-to-box application is higher than the Inbox application.
- One CUBE must have lower IPs across all the three interfaces on the same CUBE platform. For instance, CUBE-1 must have lower IP addresses in Gig0/0/0 interface compared with CUBE-2 Gig0/0/0 interface.
- CUBE box-to-box high availability requires same priority and threshold to be configured on both CUBE-1 and CUBE-2.

Configure CUBE High Availability on Cisco 4000 Series ISR and Cisco Catalyst 8000 Series Edge Platforms

Prerequisites

Ensure that you have the required licenses for configuring high availability. For detailed information, see [Cisco Unified Border Element Data Sheet](#).

- Connect the active and the standby router through a layer 2 connection for the control path.
- Configure the Network Time Protocol (NTP) or set the clock to be identical on both active and standby routers, to allow timestamps and call timers to match.



Note If switching network is of ACI, its recommended to deploy a L3 switch between CUBE HA and ACI and connect CUBE HA the L3 switch.

- The latency times must be minimal on all control and data links to prevent timeouts.
- Physically redundant links, such as Gigabit EtherChannel, must be used for the control and data paths.

Configure High Availability

Please note that the IPv6 configuration for high availability is supported for Cisco IOS XE Dublin 17.12.1a and later releases. IPv6 doesn't support redundancy control and data links, but only IPv4 supports.

SUMMARY STEPS

1. Configure the Redundancy Group (RG).
2. Configure interface tracking.
3. Configure the interfaces.
4. Configure SIP UA.
5. Configure SIP Binding.
6. Configure the Punt Policing feature.
7. Configure the RG group under **voice service voip**. This enables Box-to-box CUBE HA.
8. Configure the Media Inactivity timer.
9. Reload the router.
10. Configure the peer router.
11. Point the attached devices to the CUBE Virtual IP (VIP) address.

DETAILED STEPS

Step 1 Configure the Redundancy Group (RG).

- a) Enter application redundancy mode.

Example:

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode none
Router(config-red)#application redundancy
Router(config-red-app)#group 1
```

- b) Configure a name for the redundancy group.

Example:

```
Router(config-red-app-grp)#name cube-ha
```

where *cube-ha* is the name of the redundancy group.

- c) Specify the initial priority and failover threshold for a redundancy group.

Example:

```
Router(config-red-app-grp)#priority 100 failover threshold 75
```

where 100 is the priority value and 75 is the threshold value. Both routers should have the same priority and threshold values.

- d) Configure the timers for delay and reload.

Example:

```
Router(config-red-app-grp)#timers delay 30 reload 60
```


Delay timer which is the amount of time to delay the RG group initialization and role negotiation after the interface comes up.

Default: 30 seconds. Range is 0-10000 seconds.

Reload timer is the amount of time to delay RG group initialization and role-negotiation after a reload.

Default: 60 seconds. Range is 0-10000 seconds.

- e) Configure the interface used to exchange keepalive and hello messages between the router pair.

Example:

```
Router(config-red-app-grp)#control GigabitEthernet0/0/2 protocol 1
```

where GigabitEthernet0/0/2 is the interface and protocol 1 is the protocol instance that is attached to the interface.

- f) Configure the interface that is used for data traffic checkpoints.

Example:

```
Router(config-red-app-grp)#data GigabitEthernet0/0/2
```

Note Only IPv4 supports control and data link.

- g) Configure RG group tracking.

Example:

```
Router(config-red-app-grp)#track 1 shutdown  
Router(config-red-app-grp)#track 2 shutdown
```

- h) Specify the protocol instance that attaches to a control interface and enters redundancy application protocol configuration mode.

Example:

```
Router(config-red-app-grp)#protocol 1
```

- i) Configure the two timers for hellotime and holdtime.

Example:

```
Router(config-red-app-grp)#timers hellotime 3 holdtime 10
```

hellotime—Interval between successive hello messages.

Default is 3 seconds. Range is 250 milliseconds—254 seconds.

holdtime—The interval between the receipt of a hello message and the presumption that the sending router has failed. This duration has to be greater than the hellotime.

Default is 10 seconds. Range is 750 milliseconds—255 seconds.

We recommend that you configure the holdtime timer configured to be at least three times the value of the hellotime timer.

Step 2 Configure interface tracking.

The **track** command is used in RG to track the voice traffic interface state so that the active router initiates switchover after the traffic interface is down.

Configure the following commands at the global level to track the status of the interface.

Example:

```
Router(config)#track 1 interface GigabitEthernet0/0/0 line-protocol
Router(config)#track 2 interface GigabitEthernet0/0/1 line-protocol
```

Step 3 Configure the interfaces.

- a) Configure the redundancy interface identifier for the redundancy group.

Required for generating a Virtual MAC (VMAC) address. You must use the same rii ID value on the interface of each router (active and standby) that has the same Virtual IP address.

If there is more than one box-to-box HA pair on the same LAN, each pair MUST have unique rii IDs on their respective interfaces (to prevent collision). **show redundancy application group all** must indicate the correct local and peer information.

Example:

```
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 10.1.20.135 255.255.0.0
Router(config-if)#ipv6 address 2001:10:1:20::135/64
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 1
```

- b) Associate the interface with the redundancy group created. Following are the examples for IPv4 and IPv6 configurations:

Example:

```
Router(config-if)# redundancy group 1 ip 10.1.40.250 exclusive
Router(config-if)# redundancy group 1 ipv6 2001:10:1:40::250/64 exclusive
```

- c) Configure interface for RG control and data.

Note Only IPv4 supports redundancy control and data link.

Example:

```
Router(config)#interface GigabitEthernet0/0/2
Router(config-if)#ip address 10.1.20.113 255.255.255.0
Router(config-if)#ipv6 address 2001:10.1.20::113/64
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
```

Step 4 Configure SIP UA.

Configure the protocol mode. Supported protocol modes are IPv4, IPv6, and dual-stack configurations. IPv6 traffic flow and dual-stack for IPv4 to IPv6 interworking requires protocol mode configurations.

Example:

```
sip-ua
transport tcp tls v1.2
protocol mode ipv6
!
```

Step 5 Configure SIP Binding.

Configure CUBE to bind SIP messages to the interface that is configured with a Virtual IP address (VIP) for the RG group employed. The following example illustrates IPv4 SIP binding configurations:

Example:

```

Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number 2000
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#codec g711ulaw
Router(config-dial-peer)#!

```

```

Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 2000
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:203.0.113.13
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/1
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/1
Router(config-dial-peer)#codec g711ulaw

```

Note The following example illustrates IPv6 configuration for high availability that is supported starting from Cisco IOS XE Dublin 17.12.1a release:

Example:

```

Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number 2000
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/0
ipv6-address 2001:10:1:20::145/64
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/0 ipv6-address
 2001:10:1:20::145/64
Router(config-dial-peer)#codec g711ulaw
Router(config-dial-peer)#!

```

```

Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 2000
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv6:[2001:10:1:40:250:56ff:fe89:b7a]:2001
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/1
ipv6-address 2001:10:1:20::101/64
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/1 ipv6-address
 2001:10:1:20::101/64
Router(config-dial-peer)#codec g711ulaw

```

Step 6 Configure the Punt Policing feature.

SIP packets towards the virtual IP address and physical IP address match different punt-cause codes. The punt-rate of the virtual IP address with a punt-cause of 60, is lower than the punt-rate of the physical IP address.

To ensure that the behaviour of the SIP packets towards virtual and physical IP address remains the same, you must increase the punt-rate of the virtual IP address by using the **platform punt-policer** command in global configuration mode.

Note For Cisco IOS XE Releases 16.6.7, 16.9.4, 16.11.1, 16.12.1, 17.1.1 and later releases, you do not need to increase the punt-rate.

Example:

```

Router(config)# platform punt-policer 60 40000

```

In the preceding example, the punt-rate of the virtual IP address (punt-cause 60) is increased from the default value of 2000 to 40000.

The following table provides details of the fields of the CLI.

Table 93: CLI Fields

Keyword	Description
platform punt-policer	Configures the Punt Policing feature.
<i>60</i>	<i>punt-cause</i> —Punt cause. Range is 1–107. Punt cause of the virtual interface is 60.
<i>40000</i>	<i>punt-rate</i> —Rate limit in packets per second. Range is 10–146484.

Note The default punt rate value of the virtual IP address and the physical IP address varies with the router platform.

Note The default and maximum setting are platform specific. Default value is optimal for most deployments. Change the rate only when suggested by Cisco Support.

Step 7 Configure the RG group under **voice service voip**. This enables Box-to-box CUBE HA.

Example:

```
Router#voice service voip
Router(conf-voi-serv)#redundancy-group 1
```

Step 8 Configure the Media Inactivity timer.

The Media Inactivity Timer enables the active and standby router pair to monitor and disconnect calls if no Real-Time Protocol (RTP) packets are received within a configurable time period.

For the SIP calls, the switched over calls are cleared with signaling (as signaling information is preserved for switched calls).

The Media Inactivity Timer releases TCP-based and H.323-based calls. This is used to guard against any hung sessions resulting from the failover when a normal call disconnect does not clear the call.

You must configure the same duration for the Media Inactivity Timer on both routers. The default value is 30 seconds for SIP calls. The sample configuration is as follows:

Example:

```
Router(config)#ip rtcp report interval 9000
Router(config)#gateway
Router(config-gateway)#media-inactivity-criteria all
Router(config-gateway)#timer receive-rtp 1200
Router(config-gateway)#timer receive-rtcp 5
```

SIP call legs are cleared once the RTCP timer expires.

Step 9 Reload the router.

Once all the preceding configurations are completed, you must save the configurations, and reload the router.

Example:

```
Router>enable
Router#relaod
```

Step 10 Configure the peer router.

Follow the preceding steps to configure the standby router. Make sure that you use the correct IP addresses.

Step 11 Point the attached devices to the CUBE Virtual IP (VIP) address.

The IP-PBX, Unified SIP Proxy, or service provider must route the calls to CUBE's Virtual IP address.

HA configuration does not handle SIP messages to the CUBE's physical IP addresses.

- a. Go to **System** menu, and choose **Service Parameters**. At the bottom of the Service Parameters, enable **Advanced**.
- b. Set the **Allow TCP KeepAlives for SIP** to False.
- c. After this setting is saved, restart the CallManager Services.

Configuration Examples

Example: Control Interface Protocol Configuration

```
Router#configure terminal
Router(config)#redundancy
Router(config-red)#mode none
Router(config-red)#application redundancy
Router(config-red-app)#protocol 4
Router(config-red-app-prot)#name rg1
Router(config-red-app-prot)#timers hellotime 3 holdtime 10
Router(config-red-app-prot)#authentication text password
```

Example: Redundancy Group Protocol Configuration

```
Router#configure terminal
Router(config)#redundancy
Router(red)#application redundancy
Router(config-red-app)#protocol 1
Router(config-red-app-prtcl)#name RG1
Router(config-red-app-prtcl)#timers hellotime 1 holdtime 3
Router(config-red-app-prtcl)#end
Router#configure terminal
Router(config)#redundancy
Router(red)#application redundancy
Router(config-red-app)#protocol 2
Router(config-red-app-prtcl)#name RG1
Router(config-red-app-prtcl)#end
```

Example: Redundant Traffic Interface Configuration

Following is an example for IPv6 configuration for high availability that is supported starting from Cisco IOS XE Dublin 17.12.1a.

```
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0/2
Router(config-if)#ip address 10.1.20.113 255.0.0.0
Router(config-if)#ipv6 address 2001:10.1.20::113/64
Router(config-if)#ip nat outside
Router(config-if)#ip virtual-reassembly
```

```
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 200
Router(config-if)#redundancy group 1 ip 10.1.20.153 exclusive decrement 10
Router(config-if)#redundancy group 1 ipv6 2001:10:1:20::153/64 exclusive
```

Verify Your Configuration

All configuration commands in this task are optional. You can use the **show** commands in any order.

SUMMARY STEPS

1. **show redundancy application group** [*group-id* | **all**]
2. **show redundancy application transport** {*clients* | **group** [*group-id*]}
3. **show redundancy application protocol** {*protocol-id* | **group** [*group-id*]}
4. **show redundancy application faults group** [*group-id*]
5. **show redundancy application if-mgr group** [*group-id*]
6. **show redundancy application control-interface group** [*group-id*]
7. **show redundancy application data-interface group** [*group-id*]

DETAILED STEPS

Step 1 **show redundancy application group** [*group-id* | **all**]

Example:

```
Router#show redundancy application group
Group ID   Group Name           State
-----
1          Generic-Redundancy-1 STANDBY
2          Generic-Redundancy2  ACTIVE
```

The following example shows the details of redundancy application group 1:

```
Router#show redundancy application group 1
Group ID:1
Group Name:Generic-Redundancy-1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE
```

The following example shows the details of redundancy application group 2:

```
Router#show redundancy application group 2
Group ID:2
Group Name:Generic-Redundancy2
```

```

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

```

```

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT

```

Step 2 `show redundancy application transport {clients | group [group-id]}`

Example:

```
Router#show redundancy application transport client
```

Client	Conn#	Priority	Interface	L3	L4
(0)RF	0	1	CTRL	IPV4	SCTP
(1)MCP_HA	1	1	DATA	IPV4	UDP_REL
(4)AR	0	1	ASYM	IPV4	UDP
(5)CF	0	1	DATA	IPV4	SCTP

The following example shows configuration details for the redundancy application transport group:

```
Router#show redundancy application transport group
```

```

Transport Information for RG (1)
Client = RF
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
0   0       1.1.1.1          59000  1.1.1.2          59000  CTRL IPV4  SCTP
Client = MCP_HA
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
1   1       9.9.9.2          53000  9.9.9.1          53000  DATA IPV4  UDP_REL
Client = AR
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
2   0       0.0.0.0          0      0.0.0.0          0      NONE_IN NONE_L3 NONE_L4
Client = CF
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
3   0       9.9.9.2          59001  9.9.9.1          59001  DATA IPV4  SCTP
Transport Information for RG (2)
Client = RF
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
8   0       1.1.1.1          59004  1.1.1.2          59004  CTRL IPV4  SCTP
Client = MCP_HA
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
9   1       9.9.9.2          53002  9.9.9.1          53002  DATA IPV4  UDP_REL
Client = AR
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
10  0       0.0.0.0          0      0.0.0.0          0      NONE_IN NONE_L3 NONE_L4
Client = CF
TI  conn_id my_ip          my_port peer_ip          peer_por intf  L3  L4
11  0       9.9.9.2          59005  9.9.9.1          59005  DATA IPV4  SCTP

```

The following example shows the configuration details of redundancy application transport group 1:

```
Router#show redundancy application transport group 1
```

```
Transport Information for RG (1)
```

```

Client = RF
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
0   0       1.1.1.1        59000  1.1.1.2          59000  CTRL  IPV4   SCTP
Client = MCP_HA
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
1   1       9.9.9.2                53000  9.9.9.1          53000  DATA  IPV4   UDP_REL
Client = AR
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
2   0       0.0.0.0                0      0.0.0.0          0      NONE_IN NONE_L3 NONE_L4
Client = CF
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
3   0       9.9.9.2                59001  9.9.9.1          59001  DATA  IPV4   SCTP

```

The following example shows configuration details of redundancy application transport group 2:

```

Router#show redundancy application transport group 2
Transport Information for RG (2)
Client = RF
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
8   0       1.1.1.1                59004  1.1.1.2          59004  CTRL  IPV4   SCTP
Client = MCP_HA
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
9   1       9.9.9.2                53002  9.9.9.1          53002  DATA  IPV4   UDP_REL
Client = AR
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
10  0       0.0.0.0                0      0.0.0.0          0      NONE_IN NONE_L3 NONE_L4
Client = CF
TI  conn_id my_ip          my_port peer_ip          peer_por intf    L3    L4
11  0       9.9.9.2                59005  9.9.9.1          59005  DATA  IPV4   SCTP

```

Step 3 show redundancy application protocol {protocol-id | group [group-id]}

Example:

```

Router#show redundancy application protocol group

RG Protocol RG 1
-----
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 1.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
-----
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 117, Bytes 7254, HA Seq 0, Seq Number 117, Pkt Loss 0

```



```

Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 115, Bytes 3910, HA Seq 0, Seq Number 1453975, Pkt Loss 0

```

```

RG Protocol RG 2
-----
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 1.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

```

```

RG Media Context for RG 2
-----
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 118, Bytes 7316, HA Seq 0, Seq Number 118, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 102, Bytes 3468, HA Seq 0, Seq Number 1453977, Pkt Loss 0

```

The following example shows configuration details for the redundancy application protocol group 1:

```
Router#show redundancy application protocol group 1
```

```

RG Protocol RG 1
-----
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 1.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1

```

```

-----
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 120, Bytes 7440, HA Seq 0, Seq Number 120, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 118, Bytes 4012, HA Seq 0, Seq Number 1453978, Pkt Loss 0

```

The following example shows configuration details for the redundancy application protocol group 2:

```

Router# show redundancy application protocol group 2

RG Protocol RG 2
-----
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 1.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
-----
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 123, Bytes 7626, HA Seq 0, Seq Number 123, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 107, Bytes 3638, HA Seq 0, Seq Number 1453982, Pkt Loss 0

```

The following example shows configuration details for the redundancy application protocol 1:

```

Router#show redundancy application protocol 1

Protocol id: 1, name: rg-protocol-1
Hello timer in msec: 3000
Hold timer in msec: 10000
OVL1-1#show redundancy application protocol 2

```

```
Protocol id: 2, name: rg-protocol-2
Hello timer in msec: 3000
Hold timer in msec: 10000
```

Step 4 **show redundancy application faults group** [*group-id*]

Example:

```
Router#show redundancy application faults group

Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The following example shows configuration details specific to redundancy application faults group 1:

```
Router#show redundancy application faults group 1

Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

The following example shows configuration details specific to redundancy application faults group 2:

```
Router#show redundancy application faults group 2

Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

Step 5 **show redundancy application if-mgr group** [*group-id*]

Example:

```
Router#show redundancy application if-mgr group

RG ID: 1
=====

interface      GigabitEthernet0/0/3.152
-----
VMAC           0007.b421.4e21
VIP            55.1.1.255
Shut           shut
Decrement      10

interface      GigabitEthernet0/0/2.152
-----
VMAC           0007.b421.5209
VIP            45.1.1.255
Shut           shut
Decrement      10
```

```

RG ID: 2
=====

interface      GigabitEthernet0/0/3.166
-----
VMAC           0007.b422.14d6
VIP            4.1.255.254
Shut           no shut
Decrement      10

interface      GigabitEthernet0/0/2.166
-----
VMAC           0007.b422.0d06
VIP            3.1.255.254
Shut           no shut
Decrement      10

```

The following examples shows configuration details for redundancy application interface manager group 1 and group 2:

Router#**show redundancy application if-mgr group 1**

```

RG ID: 1
=====

interface      GigabitEthernet0/0/3.152
-----
VMAC           0007.b421.4e21
VIP            55.1.1.255
Shut           shut
Decrement      10

interface      GigabitEthernet0/0/2.152
-----
VMAC           0007.b421.5209
VIP            45.1.1.255
Shut           shut
Decrement      10

```

Router#**show redundancy application if-mgr group 2**

```

RG ID: 2
=====

interface      GigabitEthernet0/0/3.166
-----
VMAC           0007.b422.14d6
VIP            4.1.255.254
Shut           no shut
Decrement      10

interface      GigabitEthernet0/0/2.166
-----
VMAC           0007.b422.0d06
VIP            3.1.255.254
Shut           no shut
Decrement      10

```

Step 6 **show redundancy application control-interface group** [*group-id*]

Example:

```
Router#show redundancy application control-interface group
```

```
The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2
```

```
The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2
```

The following example shows configuration details of the redundancy application control-interface group 1:

```
Router#show redundancy application control-interface group 1
```

```
The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2
```

The following example shows configuration details of the redundancy application control-interface group 2:

```
Router#show redundancy application control-interface group 2
```

```
The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
Interface Neighbors:
Peer: 1.1.1.2 Active RGs: 1 Standby RGs: 2
```

Step 7 `show redundancy application data-interface group [group-id]`

Example:

```
Router#show redundancy application data-interface group
```

```
The data interface for rg[1] is GigabitEthernet0/0/1
The data interface for rg[2] is GigabitEthernet0/0/1
```

The following examples show configuration details specific to redundancy application data-interface group 1 and group 2:

```
Router#show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/0/1
```

```
Router#show redundancy application data-interface group 2
The data interface for rg[2] is GigabitEthernet0/0/1
```

Tips to Troubleshoot

Use the following show and debug commands to troubleshoot any issues:

- `show redundancy application group all`
- `show redundancy application transport clients`

- **show redundancy client domain all | inc VOIP RG**
- **show voice high-availability summary**
- **show voip fpi stats**
- **debug voip rtp session**
- **debug voice high-availability all**
- **debug voip fpi all**
- **debug redundancy application group {config | faults | media | protocol | rii transport | vp}**



Note Do not turn on a large number of debugs on a system carrying high volume of active call traffic.



CHAPTER 67

High Availability on Cisco ASR 1000 and Cisco Catalyst 8000 Series Routers

- [Feature Information, on page 757](#)
- [Overview, on page 757](#)
- [Considerations and Restrictions, on page 762](#)
- [Configure CUBE High Availability on Cisco ASR 1000 and Cisco Catalyst 8000 Series Routers, on page 764](#)
- [Verify Your Configuration, on page 778](#)
- [Tips to Troubleshoot, on page 785](#)

Feature Information

Table 94: Feature Information

Feature Name	Releases	Feature Information
High Availability Support on Cisco Unified Border Element (CUBE)	Baseline Functionality	CUBE supports redundancy and failover capability on active and standby routers.
IPv6 flows in High Availability	Cisco IOS XE Dublin 17.12.1a	The support for IPv6 flows in high availability is introduced.

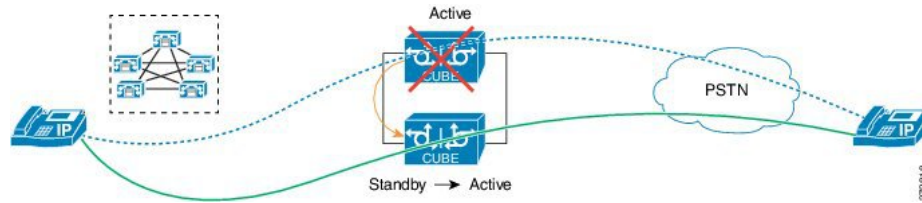
Overview



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

The High Availability (HA) feature allows you to benefit from the failover capability of Cisco Unified Border Element (CUBE) on two routers, one active and one standby. When the active router goes down for any reason, the standby router takes over seamlessly, preserving and processing your calls.

Figure 60: CUBE High Availability



CUBE supports two HA options on the Cisco ASR 1000 Series Aggregation Services Router:

- Box-to-box Redundancy
- Inbox Redundancy

The following table describes the Cisco ASR 1000 Series Router models supported for each redundancy type:

Table 95: Redundancy Type, Supported Models, and Supported Cisco IOS XE Release

Redundancy Type	Router Models	Supported Cisco IOS-XE Release
Box-to-box	<ul style="list-style-type: none"> • Cisco ASR 1001-X Router • Cisco ASR 1002-X Router • Cisco ASR 1004 Router • Cisco ASR 1006 Router (with a single RP and an ESP) • Cisco ASR 1006-X Router (with a single RP and an ESP) 	Cisco IOS XE Release 3.11 onwards
Inbox	Cisco ASR 1006 Router	Cisco IOS XE Release 3.11 onwards



Note Cisco ASR 1006 supports both Box-to-box and Inbox redundancy. You cannot switch between these two modes dynamically.

The following table provides details on the type of information that is preserved in different call types:

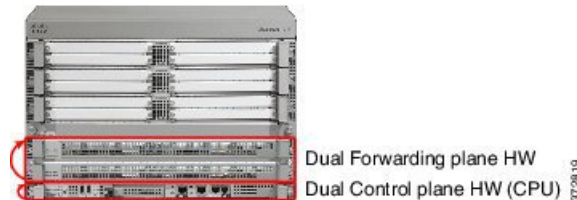
Table 96: Call Preservation for Various Call Types

Call Type	Transport Layer	Call Preservation After Switchover
SIP-SIP	UDP	Both media and session signaling are preserved.
SIP-SIP	TCP/TLS	Both media and session signaling are preserved using port 5060.

Inbox Redundancy

Inbox redundancy with Stateful Switchover (SSO) mechanism provides redundancy within the same device. Cisco ASR1006 supports the stateful failover from an active Enhanced Services Processor (ESP) to a standby and from an active Route Processor to a standby on the same box.

Figure 61: Inbox Redundancy



Box-to-Box Redundancy

Box-to-box redundancy enables configuring a pair of routers to act as back up for each other. In the router pair, the active router is determined based on the failover conditions. The router pair continuously exchange status messages. CUBE session information is checkpointed across the active and standby router. This enables the standby router to immediately take over all CUBE call processing responsibilities when the active router becomes unavailable.

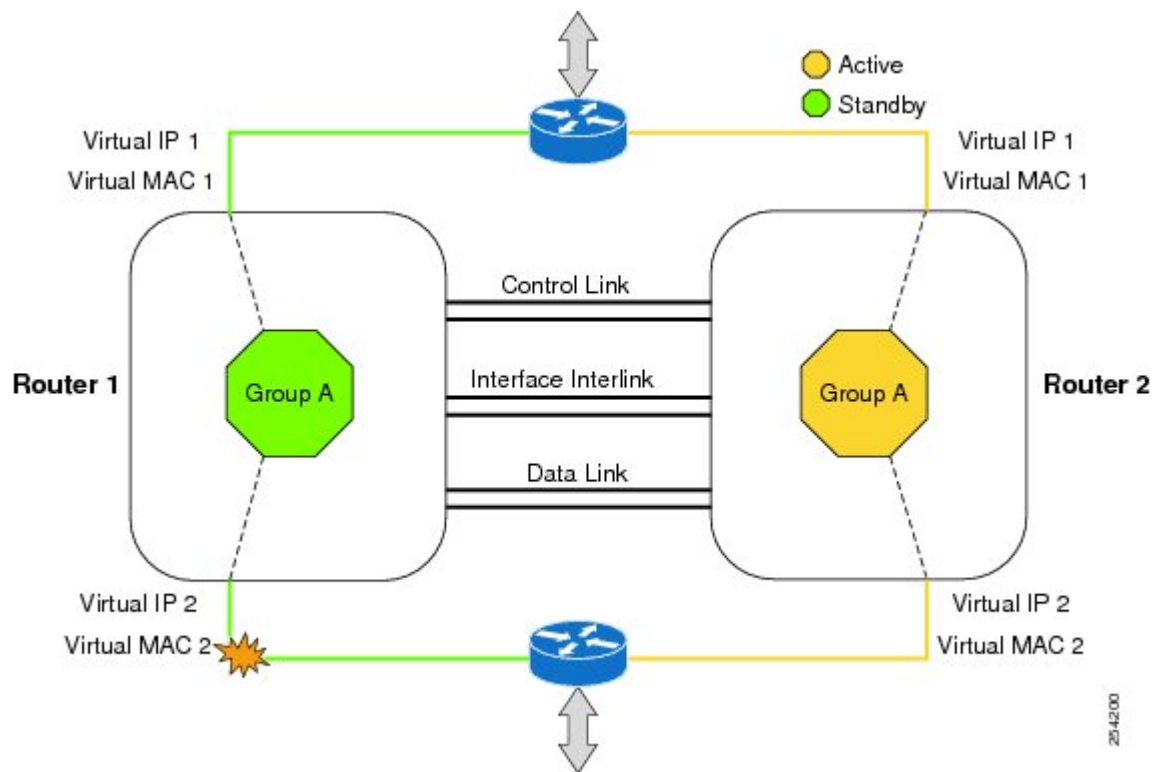
Redundancy Group (RG) Infrastructure

A group of redundant interfaces form a Redundancy Group. The active and standby routers are connected by a configurable control link and data synchronization link. The control link is used to communicate the redundancy state for each router. The data synchronization link is used to transfer stateful information to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces is configured with the same unique ID number, also known as the Redundancy Interface Identifier (RII).

A Virtual IP address (VIP) is configured on interfaces that connect to the external network. All signaling and media is sourced from and sent to the Virtual IP address. External devices such as Cisco Unified Communication Manager, uses VIP as the destination IP address for the calls traversing through CUBE.

The following figure shows the redundancy group configured for a pair of routers with a single outgoing interface.

Figure 62: Redundancy Group Configuration



PROTECTED Mode

The default failover redundancy behavior in a box-to-box HA pair is to reload the affected router to avoid out-of-sync conditions or Split brain. From release IOS XE 3.11 onwards, you can configure a Cisco ASR 1000 Series Router to transition into PROTECTED mode, which has the following features:

- Bulk sync request, Call checkpointing, and incoming call processing are disabled.
- You must manually reload a router in PROTECTED mode to come out of this state.

To enable the PROTECTED mode, use the **no redundancy-reload** command under **voice service voip**.

Network Topology

This section describes how to configure the following network topology, in which an active and standby pair of routers is used in a SIP trunk deployment between a Cisco Unified Communications Manager (Unified CM) and a service provider (SP) SIP trunk for PSTN access.

In this topology, both active and standby routers have the same configuration and both platforms are connected through a physical switch across same interfaces. This is required for CUBE HA to work. For example, the CUBE-1 and CUBE-2 interface towards WAN must terminate on the same switch. Multiple interfaces or sub-interfaces can be used on either LAN or WAN side. Also, one CUBE has a lower IP address across all three interfaces on the same CUBE platform.

We recommend that you keep the following in mind when configuring this topology:

- Connect the redundancy group control and data interfaces in the CUBE HA pair to the same physical switch to avoid any latency in the network.
- The RG control and data interfaces of the CUBE HA pair can be connected through a back-to-back cable or using a switch as shown in the following figures:

Figure 63: Network Topology with switch between active and standby routers

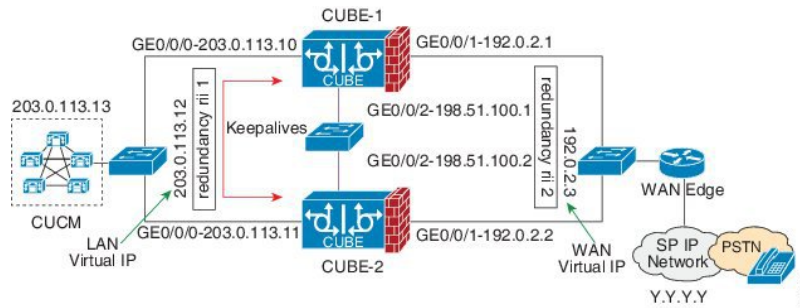
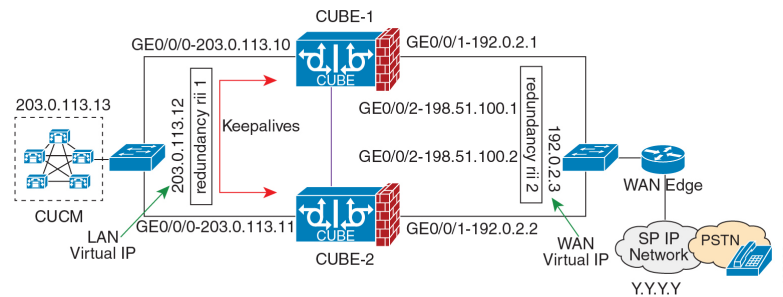


Figure 64: Network Topology with crossover cable between active and standby routers



Note However, it is recommended to use Portchannel for the RG control and data interfaces for redundancy. A single connection using back-to-back cable or switch presents a single point of failure due to a faulty cable, port, or switch, resulting in error state where both routers are Active.

- If the RG ID is the same for the two different CUBE HA pairs, keepalive interface for check-pointing the RG control and data, and traffic must be in a different subnet or VLAN.



Note This recommendation is applicable only if you connect using a switch, not by back-to-back cables.

- You can configure a maximum of two redundancy groups. Hence, there can be only two Active and Standby pairs within the same network.



Note This recommendation is applicable only if you connect using a switch, not by back-to-back cables.

- Source all signaling and media from and to the Virtual IP address.
- Always save the running configuration to avoid losing it due to router reload during a failover.
- Virtual Routing and Forwarding
 - Define Virtual Router Forwarding (VRF) in the same order on both active and standby routers for an accurate synchronization of data.
 - You can configure VRFs only on Traffic interfaces (SIP and RTP). Do not configure VRF on RG Control and Data interface.
 - VRF configurations on both the active and standby router must be identical. VRF IDs are checkpointed for the calls before and after switchover (includes VRF-based RTP port range).
- Manually copy the configurations from one router to the other.
- Replicating the configuration on the Standby router does not commit to the startup configuration; it is in the running configuration. You must run the **write memory** command to commit the changes that are synchronized from the active router on the standby router.

Considerations and Restrictions

The following is a list of further considerations and restrictions you should know before configuring this topology:

Considerations

- The same platform and configurations including interface must be used for the Active and Standby routers.
- IPv6 flows in high availability is supported starting from Cisco IOS XE Dublin 17.12.1a release.
- Only active calls are checkpointed (Calls that are connected with 200 OK or ACK transaction completed).
- When you apply and save the configuration for the first time, the platform must be reloaded.
- If you have Cisco Unified Customer Voice Portal (CVP) in your network, we recommend that you configure TCP session transport for the SIP trunk between CVP and CUBE.
- Upon failover, the previously active CUBE reloads by design.
- Smart Licensing communications happen through an active CUBE.
- Transport layer sessions (TCP/TLS/UDP) are not check-pointed between high availability pair and check will not be preserved.

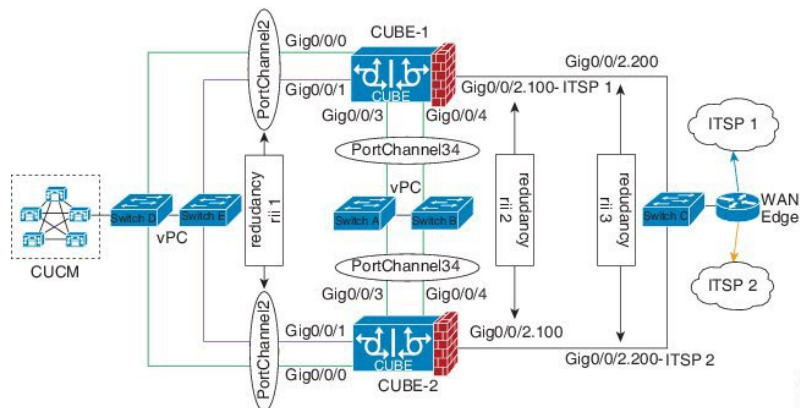
- TCP sessions are not preserved during the failover. Remote user agents are expected to reestablish TCP sessions (using port 5060 or 5061) before sending subsequent messages.
- Call Admission Control (CAC) state is maintained through switchover. After Stateful Switchover, no calls are allowed if the CAC limit is reached before the switchover.
- Up to six multimedia lines in the SDP are checkpointed for CUBE high availability. From Cisco IOS XE Release 3.17 onwards, SDP Passthru (up to two m-lines) calls are also checkpointed.
- Survivability.tcl preservation is supported from Cisco IOS XE Release 3.17 onwards for Unified Customer Voice Portal (CVP) deployments.
- SRTP-RTP, SRTP-SRTP, and SRTP Passthru are supported.



Note Redundancy control traffic that is exchanged between CUBE-1 and CUBE-2 is not secured natively and displays SRTP encryption keys in cleartext. If SRTP is used, you must secure this traffic by configuring a transport IPsec tunnel between the two interfaces used as the redundancy control link.

- Port channel is supported for both RG control data and traffic interfaces only from Cisco IOS XE 16.3.1 onwards.

Figure 65: Additional Supported Options for CUBE HA



- LTI-based transcoder call flow preservation is supported from Cisco IOS XE Release 3.15 onwards and requires the same DSP module capacity on both active and standby in the same slot or subslot.
- While deploying High Availability pair with Application Centric Infrastructure (ACI), perform one of the following:
 - Disable IP data plane learning on the ACI VRF.
 - Refer to [IP Data-plane Learning](#) for details.
 - Use an intermediate Layer 3 switch between the High Availability pair and the ACI deployment. This Layer 3 switch prevents the ACI from directly learning the CUBE IP address and its associated MAC addresses.

- From release Cisco IOS-XE 3.11 onwards, upon failover, you can move the previously active CUBE to a PROTECTED state to avoid the reload.

Restrictions

- All SCCP-based media resources (Conference bridge, Transcoding, Hardware MTP, and Software MTP) are not supported.
- Cisco Unified Survivable Remote Site Telephony (Unified SRST) or TDM Gateway co-location on CUBE HA is not supported.
- Routers connected through Metropolitan Area Network (MAN) Ethernet regardless of latency are not supported.
- Out-of-band DTMF (Notify or KPML) is not supported post switchover. Only rtp-nte to rtp-nte and voice-inband to voice-inband DTMF works after the switchover.
- Media-flow around and UC Services API (Cisco Unified Communications Manager Network-Based Recording) are not supported.
- You cannot terminate Wide Area Network (WAN) on CUBE directly or Data HA on either side. Both active and standby routers must be in the same Data Center and connected to the same physical switch.
- The Courtesy Callback (CCB) feature is not supported if a callback was registered with Cisco Unified Customer Voice Portal (CVP) and then a switchover was done on CUBE.
- You cannot configure a secondary IP address for the interfaces.
- If the redundancy group ID is same for the two different CUBE HA pairs, then the keepalive interface that is used for checkpointing RG control and data traffic must be in a different subnet or VLAN.
- One CUBE must have lower IPs across all the three interfaces on the same CUBE platform. For instance, CUBE-1 must have lower IP addresses in Gig0/0/0 interface compared with CUBE-2 Gig0/0/0 interface.
- CUBE box-to-box high availability requires same priority and threshold to be configured on both CUBE-1 and CUBE-2.

Configure CUBE High Availability on Cisco ASR 1000 and Cisco Catalyst 8000 Series Routers

Before You Begin

- Use the same hardware platform, including the cards and their positioning.
- Place both active and standby routers physically in the same location, which is connected to the same Ethernet LAN.
- If there are currently dual RPs or ESPs in the Cisco ASR 1006 Router, remove the extra RP or ESP and reload the router before configuring the redundancy mode.

Ensure that you have the required licenses for configuring high availability. For detailed information, see [Cisco Unified Border Element Data Sheet](#).

In addition to an ASR1000 platform license (Advanced IP or Advanced Enterprise) and CUBE session licenses, a Firewall/NAT Stateful Inter-Chassis Redundancy License (Part number: FLSASR1-FWNAT-R) is also required for Box-to-Box High Availability configurations.

Configure Inbox High Availability

Enable inbox redundancy.

Example:

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode sso
Router(config-r)#interchassis group 1
Router(config-r)#main-cpu
Router(config-r)#standby console enable
Router(config-r)#end
Router(config)#copy run start /* This is to save the configuration */
```

Configure Box-to-Box High Availability

IPv6 configuration for high availability is supported for Cisco IOS XE Dublin 17.12.1a and later releases. IPv6 doesn't support control and data links, but IPv4 supports.

SUMMARY STEPS

1. Disable inbox and software redundancy.
2. Configure the Redundancy Group (RG).
3. Configure interface tracking.
4. Configure the interfaces.
5. Configure SIP UA.
6. Configure SIP Binding.
7. (Optional) If H.323 calls are involved, enable H.323 binding.
8. Configure the Punt Policing feature.
9. Configure the RG group under **voice service voip**. This enables Box-to-box CUBE HA.
10. Configure the Media Inactivity timer.
11. Reload the router.
12. Configure the peer router.
13. Point the attached devices to the CUBE Virtual IP (VIP) address.

DETAILED STEPS

Step 1 Disable inbox and software redundancy.

- a) Disable software redundancy.

Example:

Disable software redundancy:

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode none
```

Example:

Disable the inbox redundancy if you are using ASR1006 router:

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode rpr
```

- b) Save the running configuration to a text file in the bootflash.

Example:

```
Router>enable
Router#copy running-configuration bootflash:<filename>
```

In the preceding command, provide a name of your preference for <filename>.

- c) Force the router to go into ROMMON mode upon next reload and erase the existing configuration from the NVRAM:

Example:

```
Router>enable
Router#configure terminal
Router(config)#config-register 0x0
Router(config)#write erase
```

- d) Reload the router.

Example:

```
Router>enable
Router#reload
```

- e) At ROMMON prompt, reset the `IOSXE_Dual_IOS` variable to disable the software redundancy.

Example:

```
rommon1>IOSXE_DUAL_IOS=0
rommon2>sync
```

- f) Boot the image from the bootflash or harddisk, or from the network.

Example:

```
rommon1>boot bootflash:isr4400-universalk9.03.13.02.S.154-3.S2-ext.SPA.bin
```


- g) When the router is up, re-apply the old configuration by copying the configuration file to the running-configuration.

Example:

```
Router>enable
Router#copy bootflash:sampleconfig running-configuration
```

- h) Change the config register back to a non-zero value.

Example:

```
Router>enable
Router#Config-register 0x2102
```

Step 2

Configure the Redundancy Group (RG).

- a) Enter application redundancy mode.

Example:

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode none
Router(config-red)#application redundancy
Router(config-red-app)#group 1
```

- b) Configure a name for the redundancy group.

Example:

```
Router(config-red-app-grp)#name cube-ha
```

where *cube-ha* is the name of the redundancy group.

- c) Specify the initial priority and failover threshold for a redundancy group.

Example:

```
Router(config-red-app-grp)#priority 100 failover threshold 75
```

where 100 is the priority value and 75 is the threshold value. Both routers should have the same priority and threshold values.

- d) Configure the timers for delay and reload.

Example:

```
Router(config-red-app-grp)#timers delay 30 reload 60
```

Delay timer which is the amount of time to delay the RG group initialization and role negotiation after the interface comes up.

Default: 30 seconds. Range is 0-10000 seconds.

Reload timer is the amount of time to delay RG group initialization and role-negotiation after a reload.

Default: 60 seconds. Range is 0-10000 seconds.

- e) Configure the interface used to exchange keepalive and hello messages between the router pair.

Example:

```
Router(config-red-app-grp)#control GigabitEthernet0/0/2 protocol 1
```

where GigabitEthernet0/0/2 is the interface and protocol 1 is the protocol instance that is attached to the interface.

- f) Configure the interface that is used for data traffic checkpoints.

Example:

```
Router(config-red-app-grp)#data GigabitEthernet0/0/2
```

Note Only IPv4 supports control and data link.

- g) Configure RG group tracking.

Example:

```
Router(config-red-app-grp)#track 1 shutdown
Router(config-red-app-grp)#track 2 shutdown
```

If you want protected mode, enter the following command:

```
Router(config-red-app-grp)#track 3 shutdown
```

- h) Specify the protocol instance that attaches to a control interface and enters redundancy application protocol configuration mode.

Example:

```
Router(config-red-app-grp)#protocol 1
```

- i) Configure the two timers for hellotime and holdtime.

Example:

```
Router(config-red-app-grp)#timers hellotime 3 holdtime 10
```

hellotime—Interval between successive hello messages.

Default is 3 seconds. Range is 250 milliseconds—254 seconds.

holdtime—The interval between the receipt of a hello message and the presumption that the sending router has failed. This duration has to be greater than the hellotime.

Default is 10 seconds. Range is 750 milliseconds—255 seconds.

We recommend that you configure the holdtime timer configured to be at least three times the value of the hellotime timer.

Step 3 Configure interface tracking.

The **track** command is used in RG to track the voice traffic interface state so that the active router initiates switchover after the traffic interface is down.

Configure the following commands at the global level to track the status of the interface.

```
Router(config)#track 1 interface GigabitEthernet0/0/0 line-protocol
Router(config)#track 2 interface GigabitEthernet0/0/1 line-protocol
```

If you want protected mode, enter the following command:

```
Router(config)#track 3 interface GigabitEthernet0/0/2 line-protocol
```

Step 4 Configure the interfaces.

- a) Configure the redundancy interface identifier for the redundancy group.

Required for generating a Virtual MAC (VMAC) address. You must use the same rii ID value on the interface of each router (active and standby) that has the same Virtual IP address.

If there is more than one box-to-box HA pair on the same LAN, each pair MUST have unique rii IDs on their respective interfaces (to prevent collision). **show redundancy application group all** must indicate the correct local and peer information.

Example:

```
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 10.1.20.135 255.255.0.0
Router(config-if)#ipv6 address 2001:10:1:20::135/64
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 1
```

- b) Associate the interface with the redundancy group created. Following are the examples for IPv4 and IPv6 configurations:

Example:

```
Router(config-if)# redundancy group 1 ip 10.1.40.250 exclusive
Router(config-if)# redundancy group 1 ipv6 2001:10:1:40::250/64 exclusive
```

- c) Configure interface for RG control and data.

Note Only IPv4 supports redundancy control and data link.

Example:

```
Router(config)#interface GigabitEthernet0/0/2
Router(config-if)#ip address 10.1.20.113 255.255.255.0
Router(config-if)#ipv6 address 2001:10:1:20::113/64
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
```

Step 5

Configure SIP UA.

Configure the protocol mode. Supported protocol modes are IPv4, IPv6, and dual-stack configurations. IPv6 traffic flow and dual-stack for IPv4 to IPv6 interworking requires protocol mode configurations.

Example:

```
sip-ua
transport tcp tls v1.2
protocol mode ipv6
!
```

Step 6

Configure SIP Binding.

Configure CUBE to bind SIP messages to the interface that is configured with a Virtual IP address (VIP) for the RG group employed. The following example illustrates IPv4 SIP binding configurations:

Example:

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number 2000
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#codec g711ulaw
Router(config-dial-peer)#!

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

```

Router(config-dial-peer)#destination-pattern 2000
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:203.0.113.13
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/1
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/1
Router(config-dial-peer)#codec g711ulaw

```

Note The following example illustrates IPv6 configuration for high availability that is supported starting from Cisco IOS XE Dublin 17.12.1a release:

Example:

```

Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number 2000
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/0
ipv6-address 2001:10:1:20::145/64
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/0 ipv6-address
 2001:10:1:20::145/64
Router(config-dial-peer)#codec g711ulaw
Router(config-dial-peer)#!

Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 2000
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv6:[2001:10:1:40:250:56ff:fe89:b7a]:2001
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/1
ipv6-address 2001:10:1:20::101/64
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/1 ipv6-address
 2001:10:1:20::101/64
Router(config-dial-peer)#codec g711ulaw

```

Step 7 (Optional) If H.323 calls are involved, enable H.323 binding.

Under the interface used by H.323, configure voip-bind with its source address equal to the interface's VIP for the RG group employed.

Example:

```

Router#voice service voip
Router(conf-voi-serv)#h323
Router(conf-serv-h323)#call preserve limit-media-detection
Router(conf-serv-h323)#no h225 timeout keepalive

Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 10.1.20.115 255.255.0.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
Router(config-if)#ipv6 address 2001:10:1:20::115/64
Router(config-if)#redundancy rii 1
Router(config-if)#redundancy group 1 ip 10.1.40.113 exclusive
Router(config-if)#redundancy group 1 ipv6 2001:10:1:40::113/64 exclusive
Router(config-if)#h323-gateway voip interface
Router(config-if)#h323-gateway voip bind srcaddr 10.1.20.115

Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 10.1.20.113 255.255.255.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 2
Router(config-if)#redundancy group 1 ip 10.1.20.119 exclusive
Router(config-if)#h323-gateway voip interface

```

```
Router(config-if)#h323-gateway voip bind srcaddr 10.1.20.119
```

Step 8

Configure the Punt Policing feature.

SIP packets towards the virtual IP address and physical IP address match different punt-cause codes. The punt-rate of the virtual IP address with a punt-cause of 60, is lower than the punt-rate of the physical IP address.

To ensure that the behaviour of the SIP packets towards virtual and physical IP address remains the same, you must increase the punt-rate of the virtual IP address by using the **platform punt-policer** command in global configuration mode.

Note For Cisco IOS XE Releases 16.6.7, 16.9.4, 16.11.1, 16.12.1, 17.1.1 and later releases, you do not need to increase the punt-rate.

Example:

```
Router(config)# platform punt-policer 60 40000
```

In the preceding example, the punt-rate of the virtual IP address (punt-cause 60) is increased from the default value of 2000 to 40000.

The following table provides details of the fields of the CLI.

Table 97: CLI Fields

Keyword	Description
platform punt-policer	Configures the Punt Policing feature.
<i>60</i>	<i>punt-cause</i> —Punt cause. Range is 1–107. Punt cause of the virtual interface is 60.
<i>40000</i>	<i>punt-rate</i> —Rate limit in packets per second. Range is 10–146484.

Note The default punt rate value of the virtual IP address and the physical IP address varies with the router platform.

Note The default and maximum setting are platform specific. Default value is optimal for most deployments. Change the rate only when suggested by Cisco Support.

Step 9

Configure the RG group under **voice service voip**. This enables Box-to-box CUBE HA.

Example:

```
Router#voice service voip
Router(conf-voi-serv)#redundancy-group 1
```

For enabling protected mode:

```
Router#voice service voip
Router(conf-voi-serv)#no redundancy-reload
```

Step 10

Configure the Media Inactivity timer.

The Media Inactivity Timer enables the active and standby router pair to monitor and disconnect calls if no Real-Time Protocol (RTP) packets are received within a configurable time period.

For the SIP calls, the switched over calls are cleared with signaling (as signaling information is preserved for switched calls).

The Media Inactivity Timer releases TCP-based and H.323-based calls. This is used to guard against any hung sessions resulting from the failover when a normal call disconnect does not clear the call.

You must configure the same duration for the Media Inactivity Timer on both routers. The default value is 30 seconds for SIP calls. The sample configuration is as follows:

Example:

```
Router(config)#ip rtcp report interval 9000
Router(config)#gateway
Router(config-gateway)#media-inactivity-criteria all
Router(config-gateway)#timer receive-rtp 1200
Router(config-gateway)#timer receive-rtcp 5
```

SIP call legs are cleared once the RTCP timer expires.

Step 11 Reload the router.

Once all the preceding configurations are completed, you must save the configurations, and reload the router.

Example:

```
Router>enable
Router#relaod
```

Step 12 Configure the peer router.

Follow the preceding steps to configure the standby router. Make sure that you use the correct IP addresses.

Step 13 Point the attached devices to the CUBE Virtual IP (VIP) address.

The IP-PBX, Unified SIP Proxy, or service provider must route the calls to CUBE's Virtual IP address.

HA configuration does not handle SIP messages to the CUBE's physical IP addresses.

- a. Go to **System** menu, and choose **Service Parameters**. At the bottom of the Service Parameters, enable **Advanced**.
- b. Set the **Allow TCP KeepAlives for SIP** to False.
- c. After this setting is saved, restart the CallManager Services.

Configuration Examples

The following sample configuration for IPv4 or IPv6 flows in High Availability assumes interface Gig0/0/0 for incoming calls, outgoing calls, and for redundancy.



Note IPv6 flows in High Availability is supported for Cisco IOS XE Dublin 17.12.1a and later releases. IPv6 flows requires protocol mode configurations.

Active Router Configurations

```
Router1# show run
```

```
Building configuration...
Current configuration : 3082 bytes
!
! Last configuration change at 21:33:13 UTC Sun Sep 19 2010
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname b2bred2
!
boot-start-marker
boot system flash bootflash:asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_201008
24_091509.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
!
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
  !
logging buffered 777777777
no logging console
enable secret 5 $1$kan3$QsGBuVkgGDZgRlg4lSrsW1
!
no aaa new-model
!
!
!
ip source-route
!
!
multilink bundle-name authenticated
!
!
voice service voip
  media bulk-stats
  allow-connections h323 to h323
  allow-connections h323 to sip
  allow-connections sip to h323
  allow-connections sip to sip
  redundancy-group 1
  h323
  emptycapability
  call preserve limit-media-detection
  no h225 timeout keepalive
  h245 passthru tcsnonstd-passthru
  sip
  early-offer forced
  midcall-signaling passthru
!
!
voice iec syslog
!
!
track 1 interface GigabitEthernet0/0/0 line-protocol
track 2 interface GigabitEthernet0/0/1 line-protocol
!
```

```

!
redundancy
mode none
application redundancy
group 1
name voice-b2bha
priority 100 failover threshold 75
timers delay 30 reload 60
control GigabitEthernet0/0/0 protocol 1
data GigabitEthernet0/0/0
track 1 shutdown
track 2 shutdown
protocol 1
timers hellotime 3 holdtime 10
!
!
!
ip ftp username bhks
ip ftp password bhks
!
!
interface GigabitEthernet0/0/0
ip address 10.1.20.135 255.255.255.0
media-type rj45
negotiation auto
ipv6 address 2001:10:1:20::135/64
no mop enabled
redundancy rii 1
redundancy group 1 ip 10.1.20.155 exclusive
redundancy group 1 ipv6 2001:10:1:20::155/64 exclusive
h323-gateway voip interface
h323-gateway voip bind srcaddr 10.1.20.135
!
interface GigabitEthernet0/0/1
ip address 198.51.100.1 255.255.255.0
media-type rj45
negotiation auto
!
interface GigabitEthernet0/0/0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
!
!
no ip http server
no ip http secure-server
ip rtcp report interval 9000
ip route 0.0.0.0 0.0.0.0 9.44.0.1
!
logging esm config
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
!
control-plane
!
!
!
dial-peer voice 10 voip
destination-pattern 140854.....
session protocol sipv2
session target ipv4:y.y.y.y
voice-class sip bind control source-interface GigabitEthernet0/0/1 ipv6-address

```



```

2001:10:1:20::155
  voice-class sip bind media source-interface GigabitEthernet0/0/1 ipv6-address
2001:10:1:20::155
  codec g711ulaw
  no vad
!
dial-peer voice 20 voip
  session protocol sipv2
  session target ipv4:203.0.113.13
  session target ipv6:[2001:10:1:40:250:56ff:fe89:b7a]:2001
  incoming called-number 140854.....
  voice-class sip bind control source-interface GigabitEthernet0/0/1 ipv6-address
2001:10:1:20::155
  voice-class sip bind media source-interface GigabitEthernet0/0/1 ipv6-address
2001:10:1:20::155
  codec g711ulaw
  no vad
!
!
sip-ua
transport tcp tls v1.2
protocol mode ipv6
!
gateway
  media-inactivity-criteria all
  timer receive-rtcp 5
  timer receive-rtp 1200
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
line vty 0 4
  no login
!
exception data-corruption buffer truncate
end

```

Standby Router Configurations

```

Router2#sh run
Building configuration...
Current configuration : 2606 bytes
!
! Last configuration change at 21:34:07 UTC Sun Sep 19 2010
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname b2bred1
!
boot-start-marker
boot system flash bootflash:asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_201008
24_091509.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family

```

```

!
logging buffered 777777777
no logging console
!
no aaa new-model
!
!
ip source-route
!
!!
multilink bundle-name authenticated
!
!
!
voice service voip
  media bulk-stats
  allow-connections h323 to h323
  allow-connections h323 to sip
  allow-connections sip to h323
  allow-connections sip to sip
  redundancy-group 1
  h323
    emptycapability
    call preserve limit-media-detection
    no h225 timeout keepalive
    h245 passthru tcsnonstd-passthru
  sip
    early-offer forced
    midcall-signaling passthru
!
!
voice iec syslog
!
!
!
track 1 interface GigabitEthernet0/0/0 line-protocol
track 2 interface GigabitEthernet0/0/1 line-protocol
!
!
!
redundancy
  mode none
  application redundancy
  group 1
    name voice-b2bha
    priority 100 failover threshold 75
    timers delay 30 reload 60
    control GigabitEthernet0/0/0 protocol 1
    data GigabitEthernet0/0/0
    track 1 shutdown
    track 2 shutdown
  protocol 1
    timers hellotime 3 holdtime 10
!
!
ip ftp username bhks
ip ftp password bhks
!
!
interface GigabitEthernet0/0/0
  ip address 10.1.20.115 255.255.255.0
  media-type rj45
  negotiation auto
  ipv6 address 2001:10:1:20::115/64

```

```

redundancy rii 1
redundancy group 1 ip 10.1.20.155 exclusive
redundancy group 1 ipv6 2001:10:1:20::155/64 exclusive
h323-gateway voip interface
h323-gateway voip bind srcaddr 10.1.20.115
!
interface GigabitEthernet0/0/0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
!
no ip http server
no ip http secure-server
ip rtcp report interval 9000
ip route 0.0.0.0 0.0.0.0 9.44.0.1
!
logging esm config
!
!
control-plane
!
!
dial-peer voice 10 voip
 destination-pattern 140854.....
 session protocol sipv2
 voice-class sip bind control source-interface GigabitEthernet0/0/0 ipv6-address
 2001:10:1:20::155
 voice-class sip bind media source-interface GigabitEthernet0/0/0 ipv6-address
 2001:10:1:20::155
 codec g711ulaw
 no vad
!
dial-peer voice 20 voip
 session protocol sipv2
 session target ipv6:[2001:10:1:40:250:56ff:fe89:b7a]:2001
 incoming called-number 140854.....
 voice-class sip bind control source-interface GigabitEthernet0/0/0 ipv6-address
 2001:10:1:20::155
 voice-class sip bind media source-interface GigabitEthernet0/0/0 ipv6-address
 2001:10:1:20::155
 codec g711ulaw
 no vad
!
!
sip-ua
 transport tcp tls v1.2
 protocol mode ipv6
!
gateway
 media-inactivity-criteria all
 timer receive-rtcp 5
 timer receive-rtp 1200
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 no login
!
exception data-corruption buffer truncate
end

```

Verify Your Configuration

Verify Redundancy State on Active and Standby Routers

Use the `show redundancy application group all` command to display the redundancy inter-device states.

Step 1 Active Router:

Example:

```
Router#show redundancy application group all

Faults states Group 1 info:
  Runtime priority: [100]
  RG Faults RG State: Up.
    Total # of switchovers due to faults: 0
    Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:voice-b2bha

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
  RF state: ACTIVE
  Peer RF state: STANDBY HOT

RG Protocol RG 1
-----
  Role: Active
  Negotiation: Enabled
  Priority: 100
  Protocol state: Active
  Ctrl Intf(s) state: Up
  Active Peer: Local
  Standby Peer: address 203.0.113.11, priority 100, intf Gi0/0/2
  Log counters:
    role change to active: 1
    role change to standby: 0
    disable events: rg down state 1, rg shut 0
    ctrl intf events: up 1, down 2, admin_down 1
    reload events: local request 0, peer request 0

RG Media Context for RG 1
-----
  Ctx State: Active
  Protocol ID: 1
  Media type: Default
  Control Interface: GigabitEthernet0/0/2
  Current Hello timer: 3000
  Configured Hello timer: 3000, Hold timer: 10000
  Peer Hello timer: 3000, Peer Hold timer: 10000
  Stats:
  Pkts 27719, Bytes 1718578, HA Seq 0, Seq Number 27719, Pkt Loss
```

```

0
  Authentication not configured
  Authentication Failure: 0
  Reload Peer: TX 0, RX 0
  Resign: TX 0, RX 0
  Standby Peer: Present. Hold Timer: 10000
  Pkts 27700, Bytes 941800, HA Seq 0, Seq Number 27708, Pkt Loss 0

```

Step 2 Standby Router:

Example:

```

Router#show redundancy application group all

Faults states Group 1 info:
  Runtime priority: [100]
  RG Faults RG State: Up.
  Total # of switchovers due to faults: 0
  Total # of down/up state changes due to faults: 2
  Group ID:1
  Group Name:voice-b2bha

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
  RF state: STANDBY HOT
  Peer RF state: ACTIVE

RG Protocol RG 1
-----
  Role: Standby
  Negotiation: Enabled
  Priority: 100
  Protocol state: Standby-hot
  Ctrl Intf(s) state: Up
  Active Peer: address 203.0.113.10, priority 100, intf Gi0/0/2
  Standby Peer: Local
  Log counters:
    role change to active: 0
    role change to standby: 1
    disable events: rg down state 1, rg shut 0
    ctrl intf events: up 1, down 2, admin_down 1
    reload events: local request 0, peer request 0

RG Media Context for RG 1
-----
  Ctx State: Standby
  Protocol ID: 1
  Media type: Default
  Control Interface: GigabitEthernet0/0/2
  Current Hello timer: 3000
  Configured Hello timer: 3000, Hold timer: 10000
  Peer Hello timer: 3000, Peer Hold timer: 10000
  Stats:
    Pkts 27832, Bytes 1725584, HA Seq 0, Seq Number 27832, Pkt Loss
0
  Authentication not configured
  Authentication Failure: 0

```

```

Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 27830, Bytes 946220, HA Seq 0, Seq Number 27843, Pkt Loss 0

```

Verify Call State After Switchover

Use the **show voice high-availability summary** command to verify the following:

- The checkpointing of calls on the standby router after a switchover
- The media-inactivity count on the active router when the calls are over
- Native and non-native (preserved) calls when both call types are present
- Presence of leaked RTP, HA, SPI sessions

Active Router

```
Router#show voice high-availability summary
```

```
===== HA Message Sizes =====
```

```

SCCPAPP Data Size:412
SIPSPI Data Size:4260
H323SPI Data Size:2164
RTSPI Data Size:861
CCAPI Data Size:188
VOIP RTP Data Size:158
HA Data Size:68
Total Data Size:4842

```

```
===== Voice HA DB INFO =====
```

```

Number of calls in HA DB: 0
Number of calls in HA sync pending DB: 0
Number of current SWMTP calls with HA: 0
-----

```

```
First a few entries in HA DB:
```

```
-----
First a few entries in Sync Pending DB:
```

```
===== Voice HA Process INFO =====
```

```

Active process current tick: 92663
Active process number of tick events pending: 0
Active process number of tick events processed: 0
===== Voice HA RF INFO =====

```

```
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] :
```



```

Tick event queue overrun count: 0
Checkpoint send failure count - ISSU Transform Failure: 0
Checkpoint send failure count - CF failed: 0
Checkpoint get buffer failure count: 0
Checkpoint Received IPC Flow ON from CF: 0
Checkpoint Received IPC Flow OFF from CF: 0

```

Standby Router

```
Router#show voice high-availability summary
```

```

===== HA Message Sizes =====
SCCPAPP Data Size:412
SIPSPI Data Size:4260
H323SPI Data Size:2164
RTSPI Data Size:861
CCAPI Data Size:188
VOIP RTP Data Size:158
HA Data Size:68
Total Data Size:4842

===== Voice HA DB INFO =====
Number of calls in HA DB: 0
Number of calls in HA sync pending DB: 0
Number of current SWMTP calls with HA: 0
-----
First a few entries in HA DB:
-----
First a few entries in Sync Pending DB:
-----

===== Voice HA Process INFO =====
Active process current tick: 46846
Active process number of tick events pending: 0
Active process number of tick events processed: 0
===== Voice HA RF INFO =====
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: 418
My current RF state STANDBY HOT (8)
Peer current RF state ACTIVE (13)
Current VOIP HA state [LOCAL / PEER] :
[STANDBY HOT (8) / ACTIVE (13)]
-----
Voice HA Standby is not available.
System has not experienced switchover.

===== Voice HA CF INFO =====
Voice HA CF for RG(1):
  local ip = 203.0.113.10; remote ip = 203.0.113.11
  local port = 4025; remote port = 4026

```



```
SIP User Agent bind status(media): DISABLED
Snapshot of SIP listen sockets : 2

=====
Local Address Listen Port Secure Listen Port
=====
203.0.113.13          5060          5061
203.0.113.13          5060          5061
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
```

Verify Current CPU Use

Use the **show process cpu history** to verify the CPU utilization percentage at regular intervals.

Check CPU utilization before performing a switchover and proceed with a forced failover only when the CPU utilization is less than 70%. You can also use **show process cpu sorted** command repeatedly to know the CPU utilization for a particular process.

Force a Manual Failover for Testing

Box-to-box redundancy on the Cisco ASR 1000 Series Router platform supports full stateful switchover of calls. This means the media (RTP) and signaling information of the calls is preserved.

You can expect that switchovers occurring in real environments, where there is a constant mixture of calls in transient (call setup or being modified) and established state, result in some dropped calls during a failover.

To check that your configuration is correct, you can force a manual switchover.



Note A switchover involves the active router reloading, while the standby router takes over and becomes the new active router, processing incoming calls and maintaining the media streams and signaling information for calls until they are complete. The new active router continues to act as such until another switchover occurs. There is no pre-emption mechanism on Box-to-box redundancy.

Before you begin

Before you start a manual switchover, take note of the following:

- Monitor the CPU utilization % on the active and standby router pair. The active router has the higher CPU utilization as it is actively handling the calls, while the standby router shows little CPU utilization.
- Ensure that you perform a manual switchover when the CPU utilization of the active router is not more than 70%.
- Use the **show voip rtp connection** command to make sure that existing calls across the active and standby router pair are in sync.

You can achieve manual switchovers in various ways:

Procedure

- Initiate the manual switchover by using the CLI **redundancy application reload group *RG ID* self** on the active router.
- Reload of the active router

- Power cycle the active router
- Pull out any RG configured interface of the active router
- Shutdown any RG configured interface of the active router

Tips to Troubleshoot

Use the following show and debug commands to troubleshoot High Availability issues:

- **show redundancy application group all**
- **show redundancy application transport clients**
- **show redundancy client domain all | inc VOIP RG**
- **show voice high-availability summary**
- **show voip fpi stats**
- **debug voip rtp session**
- **debug voice high-availability all**
- **debug voip fpi all**
- **debug redundancy application group {config | faults | media | protocol | rii transport | vp}**



Note On every switchover after reload, you must enable the debugs on the new standby router.



Note Do not turn on many debugs on a system carrying high volume of active call traffic.

Troubleshooting Tips

- Check for proper HA states on both the active and standby router in the output of the show commands, like **show redundancy application group**.
- Perform incoming and outgoing ping tests with the VIPs employed.
- In the presence of active calls, look for the use of any physical interface's IP address in the output of **show voip rtp connections** on both the active and standby routers. VIP must be used in both the show outputs and the debugs.
- In the output of **show voip rtp connection | inc Found** and **show call active voice compact | inc Total** on both the active and standby routers, check for any large number of mismatched calls.
- To debug problems, enable the corresponding debug options:
 - VoIP RTP
 - VoIP FPI
 - VoIP HA

- SPIs (SIP, H.323, SCCPAPP)



CHAPTER 68

High Availability on Cisco C8000V Series Cloud Services Routers

- [Overview, on page 787](#)
- [Considerations and Restrictions, on page 792](#)
- [How to Configure vCUBE High Availability on C8000V Series Routers, on page 794](#)
- [Tips to Troubleshoot, on page 800](#)

Overview



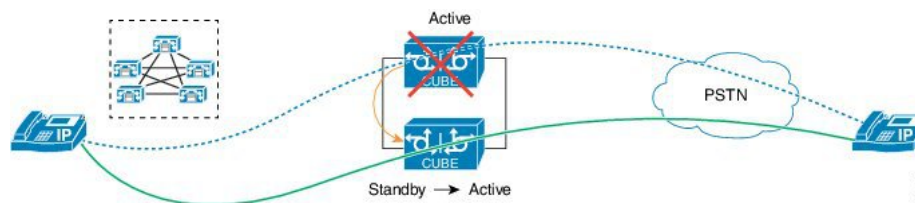
Note Cisco Cloud Services Router 1000V Series (CSR 1000V) is no longer supported from Cisco IOS XE Bengaluru 17.4.1a onwards. If you are using CSR 1000V, you have to upgrade to Cisco Catalyst 8000V Edge Software (Catalyst 8000V). For End-of-Life information on CSR 1000V, see [End-of-Sale and End-of-Life Announcement for the Select Cisco CSR 1000v Licenses](#).



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

The High Availability (HA) feature allows you to benefit from the failover capability of Cisco Unified Border Element (CUBE) on two routers, one active and one standby. When the active router goes down for any reason, the standby router takes over seamlessly, preserving and processing your calls.

Figure 66: CUBE High Availability



Cisco Unified Border Element (CUBE) running on Cisco CSR 1000v Series Cloud Services Router and C8000V is called Virtual CUBE (vCUBE). vCUBE leverages Redundancy Group (RG) Infrastructure to

provide high availability. HA is configured between two vCUBE Cisco CSR 1000v or C8000V instances running on either the same host or across different hosts that are connected through the same switch.

You can configure vCUBE Cisco CSR 1000v or C8000V on running on virtualized hosts listed in the [Cisco Unified Border Element Data Sheet](#).

Feature Information

Table 98: Feature Information

Feature Name	Releases	Feature Information
High Availability Support on Cisco Unified Border Element (CUBE)	Baseline Functionality	CUBE supports redundancy and failover capability on active and standby routers.
IPv6 flows in High Availability	Cisco IOS XE Dublin 17.12.1a	The support for IPv6 flows in high availability is introduced.

Box-to-Box Redundancy

Box-to-box redundancy enables configuring a pair of routers to act as back up for each other. In the router pair, the active router is determined based on the failover conditions. The router pair continuously exchange status messages. CUBE session information is checkpointed across the active and standby router. This enables the standby router to immediately take over all CUBE call processing responsibilities when the active router becomes unavailable.

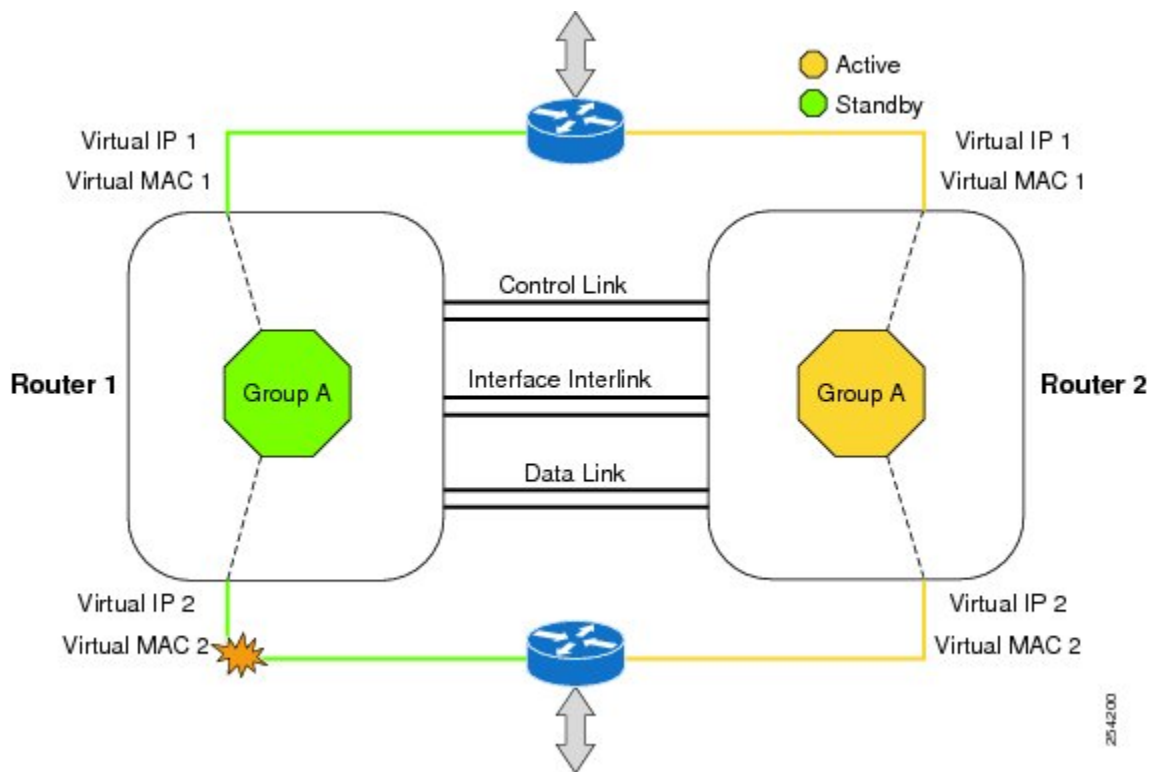
Redundancy Group (RG) Infrastructure

A group of redundant interfaces form a Redundancy Group. The active and standby routers are connected by a configurable control link and data synchronization link. The control link is used to communicate the redundancy state for each router. The data synchronization link is used to transfer stateful information to synchronize the stateful database for the calls and media flows. Each pair of redundant interfaces is configured with the same unique ID number, also known as the Redundancy Interface Identifier (RII).

A Virtual IP address (VIP) is configured on interfaces that connect to the external network. All signaling and media is sourced from and sent to the Virtual IP address. External devices such as Cisco Unified Communication Manager, uses VIP as the destination IP address for the calls traversing through CUBE.

The following figure shows the redundancy group configured for a pair of routers with a single outgoing interface.

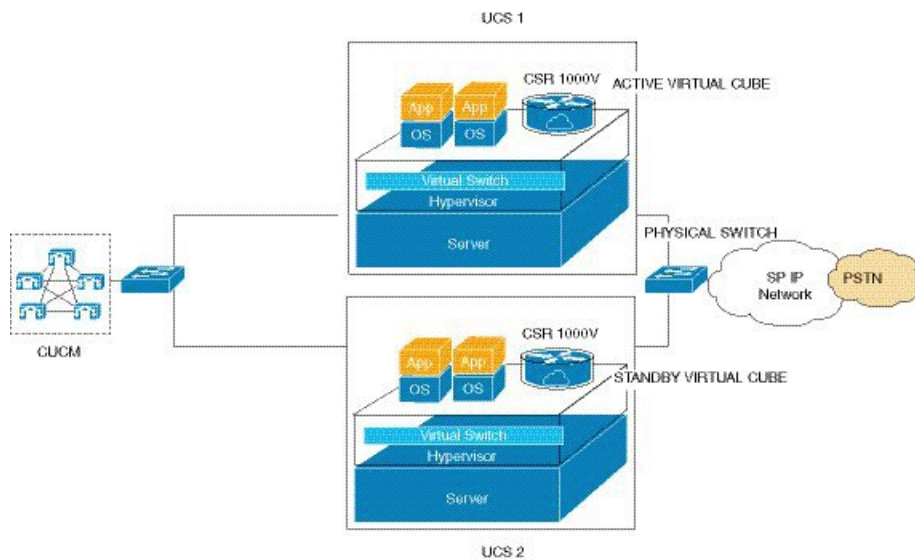
Figure 67: Redundancy Group Configuration



254200

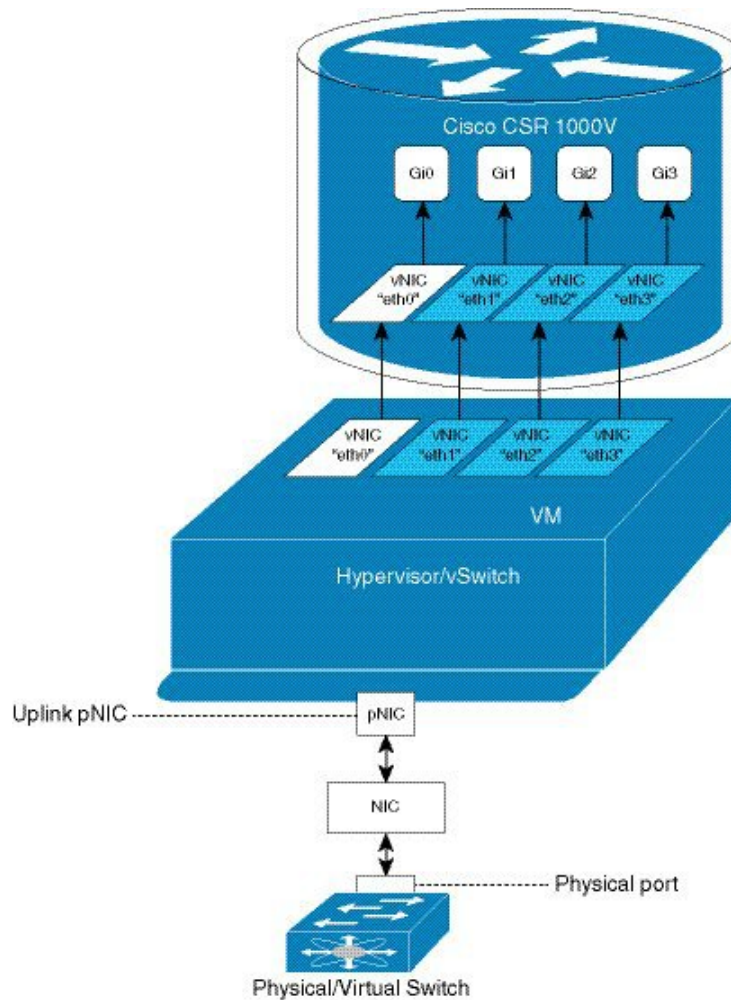
Network Topology

Figure 68: Virtual CUBE High Availability



363794

Figure 69: vNICs Mapped to Cisco CSR 1000V or C8000V Router Interfaces



We recommend that you keep the following in mind when enabling this topology:

- Connect the Cisco CSR 1000v or C8000V running on the server to the virtual switch within the virtualized host. Then connect the virtual switches to external switches using the physical host interfaces. The virtual switch routes the traffic internally between the virtual machines and also connects the external networks.
- Configure the virtual switch to propagate the status of the physical switch so that vCUBE shows the status as "down" when the interface connecting the physical switch is down. vCUBE tracks only the status of the interface connecting the virtual switch. It does not track the status of the interface connecting the physical switch. Therefore, we recommend you to configure the virtual switch to propagate the status of the physical switch.
- Configure HA connectivity using redundancy on virtual switch to avoid checkpointing failures.

In a scenario where the physical switch is down and there is no redundancy configured on virtual switch, the active router continues to process calls as it tracks only the status of virtual switch (which is up). At the same time, the standby router assumes the role of active router as it does not receive keepalive messages from the active router through the physical switch. Hence checkpointing fails. To avoid such scenarios, we recommend you to configure HA connectivity using redundancy on virtual switch.

- Do not track the switches that are used to connect non-networking end devices or LAN, to determine uplink failures.
- Connect the redundancy group control and data interfaces in the CUBE HA pair to the same physical switch to avoid any latency in the network.
- The RG control and data interfaces of the CUBE HA pair can be connected through a back-to-back cable or using a switch as shown in the following figures:

Figure 70: Network Topology with switch between active and standby routers

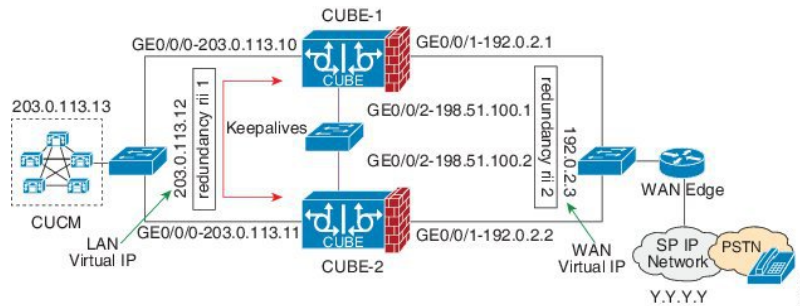
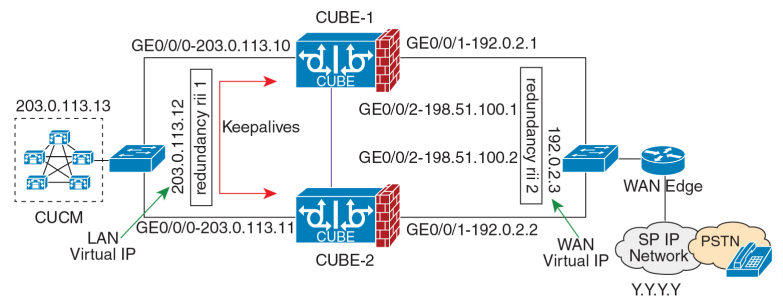


Figure 71: Network Topology with crossover cable between active and standby routers



Note However, it is recommended to use Portchannel for the RG control and data interfaces for redundancy. A single connection using back-to-back cable or switch presents a single point of failure due to a faulty cable, port, or switch, resulting in error state where both routers are Active.

- If the RG ID is the same for the two different CUBE HA pairs, keepalive interface for check-pointing the RG control and data, and traffic must be in a different subnet or VLAN.



Note This recommendation is applicable only if you connect using a switch, not by back-to-back cables.

- You can configure a maximum of two redundancy groups. Hence, there can be only two Active and Standby pairs within the same network.



Note This recommendation is applicable only if you connect using a switch, not by back-to-back cables.

- Source all signaling and media from and to the Virtual IP address.
- Always save the running configuration to avoid losing it due to router reload during a failover.
- Virtual Routing and Forwarding
 - Define Virtual Router Forwarding (VRF) in the same order on both active and standby routers for an accurate synchronization of data.
 - You can configure VRFs only on Traffic interfaces (SIP and RTP). Do not configure VRF on RG Control and Data interface.
 - VRF configurations on both the active and standby router must be identical. VRF IDs are checkpointed for the calls before and after switchover (includes VRF-based RTP port range).
- Manually copy the configurations from one router to the other.
- Replicating the configuration on the Standby router does not commit to the startup configuration; it is in the running configuration. You must run the **write memory** command to commit the changes that are synchronized from the active router on the standby router.

Considerations and Restrictions

The following is a list of further considerations and restrictions you should know before configuring this topology:

Considerations

- The same platform and configurations including interface must be used for the Active and Standby routers.
- IPv6 flows in high availability is supported starting from Cisco IOS XE Dublin 17.12.1a release.
- Only active calls are checkpointed (Calls that are connected with 200 OK or ACK transaction completed).
- When you apply and save the configuration for the first time, the platform must be reloaded.
- If you have Cisco Unified Customer Voice Portal (CVP) in your network, we recommend that you configure TCP session transport for the SIP trunk between CVP and CUBE.
- Upon failover, the previously active CUBE reloads by design.
- Smart Licensing communications happen through an active CUBE.
- Transport layer sessions (TCP/TLS/UDP) are not check-pointed between high availability pair and check will not be preserved.

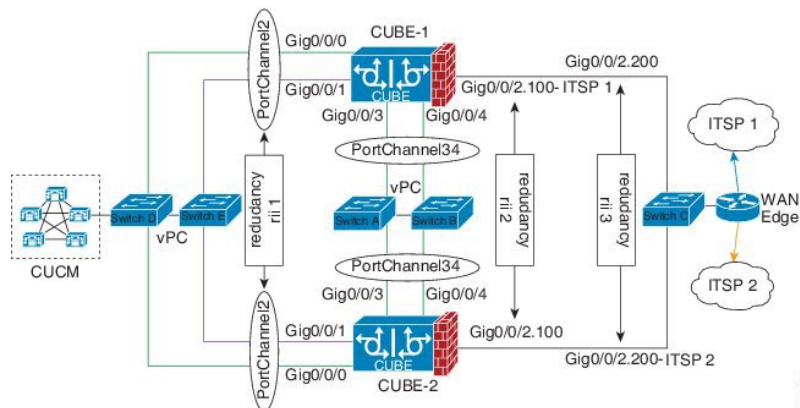
- TCP sessions are not preserved during the failover. Remote user agents are expected to reestablish TCP sessions (using port 5060 or 5061) before sending subsequent messages.
- Call Admission Control (CAC) state is maintained through switchover. After Stateful Switchover, no calls are allowed if the CAC limit is reached before the switchover.
- Up to six multimedia lines in the SDP are checkpointed for CUBE high availability. From Cisco IOS XE Release 3.17 onwards, SDP Passthru (up to two m-lines) calls are also checkpointed.
- Survivability.tcl preservation is supported from Cisco IOS XE Release 3.17 onwards for Unified Customer Voice Portal (CVP) deployments.
- SRTP-RTP, SRTP-SRTP, and SRTP Passthru are supported.



Note Redundancy control traffic that is exchanged between CUBE-1 and CUBE-2 is not secured natively and displays SRTP encryption keys in cleartext. If SRTP is used, you must secure this traffic by configuring a transport IPsec tunnel between the two interfaces used as the redundancy control link.

- Port channel is supported for both RG control data and traffic interfaces only from Cisco IOS XE 16.3.1 onwards.

Figure 72: Additional Supported Options for CUBE HA



Restrictions

- Geographic stateful switchover is not supported.
- Calls in the transient state at the time of switchover are not preserved.
- All SCCP-based media resources (Conference bridge, Transcoding, Hardware MTP, and Software MTP) are not supported.
- Cisco Unified Survivable Remote Site Telephony (Unified SRST) or TDM Gateway co-location on CUBE HA is not supported.
- Routers connected through Metropolitan Area Network (MAN) Ethernet regardless of latency are not supported.

- Out-of-band DTMF (Notify or KPML) is not supported post switchover. Only rtp-nte to rtp-nte and voice-inband to voice-inband DTMF works after the switchover.
- Media-flow around and UC Services API (Cisco Unified Communications Manager Network-Based Recording) are not supported.
- You cannot terminate Wide Area Network (WAN) on CUBE directly or Data HA on either side. Both active and standby routers must be in the same Data Center and connected to the same physical switch.
- The Courtesy Callback (CCB) feature is not supported if a callback was registered with Cisco Unified Customer Voice Portal (CVP) and then a switchover was done on CUBE.
- You cannot configure a secondary IP address for the interfaces.
- If the redundancy group ID is same for the two different CUBE HA pairs, then the keepalive interface that is used for checkpointing RG control and data traffic must be in a different subnet or VLAN.

How to Configure vCUBE High Availability on C8000V Series Routers

Prerequisite

Ensure that you have the required licenses for configuring high availability. For detailed information, see [Cisco Unified Border Element Data Sheet](#).

Configure High Availability

Please note that the IPv6 flows for High Availability is supported for Cisco IOS XE Dublin 17.12.1a and later releases. IPv6 doesn't support control and data links, but IPv4 supports.

Step 1 Configure the Redundancy Group (RG).

- a) Enter application redundancy mode.

Example:

```
Router>enable
Router#configure terminal
Router(config)#redundancy
Router(config-r)#mode none
Router(config-red)#application redundancy
Router(config-red-app)#group 1
```

- b) Configure a name for the redundancy group.

Example:

```
Router(config-red-app-grp)#name cube-ha
```

where *cube-ha* is the name of the redundancy group.

- c) Specify the initial priority and failover threshold for a redundancy group.

Example:

```
Router(config-red-app-grp)#priority 100 failover threshold 75
```

where 100 is the priority value and 75 is the threshold value. Both routers should have the same priority and threshold values.

- d) Configure the timers for delay and reload.

Example:

```
Router(config-red-app-grp)#timers delay 30 reload 60
```

Delay timer which is the amount of time to delay the RG group initialization and role negotiation after the interface comes up.

Default: 30 seconds. Range is 0-10000 seconds.

Reload timer is the amount of time to delay RG group initialization and role-negotiation after a reload.

Default: 60 seconds. Range is 0-10000 seconds.

- e) Configure the interface used to exchange keepalive and hello messages between the router pair.

Example:

```
Router(config-red-app-grp)#control GigabitEthernet2 protocol 1
```

where GigabitEthernet2 is the interface and protocol 1 is the protocol instance that is attached to the interface.

- f) Configure the interface that is used for data traffic checkpoints.

Example:

```
Router(config-red-app-grp)#data GigabitEthernet2
```

- g) Configure RG group tracking.

Example:

```
Router(config-red-app-grp)#track 1 shutdown  
Router(config-red-app-grp)#track 2 shutdown
```

- h) Specify the protocol instance that attaches to a control interface and enters redundancy application protocol configuration mode.

Example:

```
Router(config-red-app-grp)#protocol 1
```

- i) Configure the two timers for hellotime and holdtime.

Example:

```
Router(config-red-app-grp)#timers hellotime 3 holdtime 10
```

hellotime—Interval between successive hello messages.

Default is 3 seconds. Range is 250 milliseconds—254 seconds.

holdtime—The interval between the receipt of a hello message and the presumption that the sending router has failed. This duration has to be greater than the hellotime.

Default is 10 seconds. Range is 750 milliseconds—255 seconds.

We recommend that you configure the holdtime timer configured to be at least three times the value of the hellotime timer.

Step 2 Configure interface tracking.

The **track** command is used in RG to track the voice traffic interface state so that the active router initiates switchover after the traffic interface is down.

Configure the following commands at the global level to track the status of the interface.

```
Router(config)#track 1 interface GigabitEthernet0/0/0 line-protocol
Router(config)#track 2 interface GigabitEthernet0/0/1 line-protocol
```

Step 3 Configure the interfaces.

- a) Configure the redundancy interface identifier for the redundancy group.

Required for generating a Virtual MAC (VMAC) address. You must use the same rii ID value on the interface of each router (active and standby) that has the same Virtual IP address.

If there is more than one box-to-box HA pair on the same LAN, each pair **MUST** have unique rii IDs on their respective interfaces (to prevent collision). **show redundancy application group all** must indicate the correct local and peer information.

Example:

```
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 203.0.113.10 255.255.0.0
Router(config-if)#ipv6 address 2001:420:54FF:13::312:103/119
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 1
```

- b) Associate the interface with the redundancy group created. Following are the examples for IPv4 and IPv6 configurations:

Example:

```
Router(config-if)# redundancy group 1 ip 10.1.40.250 exclusive
Router(config-if)# redundancy group 1 ipv6 2001:10:1:40::250/64 exclusive
```

- c) Configure interface for RG control and data.

Only IPv4 supports redundancy control and data links.

Example:

```
Router(config)#interface GigabitEthernet0/0/2
Router(config-if)#ip address 10.1.20.113 255.255.255.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
```

Step 4 Configure SIP Binding.

Configure CUBE to bind SIP messages to the interface that is configured with a Virtual IP address (VIP) for the RG group employed. The following example illustrates IPv4 SIP binding configurations:

Example:

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#incoming called-number 2000
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/0
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/0 ipv6-address
```

```

2001:10:1:20::155
Router(config-dial-peer)#codec g711ulaw
Router(config-dial-peer)#!

Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 2000
Router(config-dial-peer)#session protocol sipv2
Router(config-dial-peer)#session target ipv4:203.0.113.13
Router(config-dial-peer)#session target ipv6:[2001:10:1:40:250:56ff:fe89:b7a]:2001
Router(config-dial-peer)#voice-class sip bind control source-interface GigabitEthernet0/0/1
ipv6-address 2001:10:1:20::155
Router(config-dial-peer)#voice-class sip bind media source-interface GigabitEthernet0/0/1 ipv6-address
2001:10:1:20::155
Router(config-dial-peer)#codec g711ulaw

```

Step 5 (Optional) If H.323 calls are involved, enable H.323 binding.

Under the interface used by H.323, configure voip-bind with its source address equal to the interface's VIP for the RG group employed.

Example:

```

Router#voice service voip
Router(conf-voi-serv)#h323
Router(conf-serv-h323)#call preserve limit-media-detection
Router(conf-serv-h323)#no h225 timeout keepalive

Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 203.0.113.10 255.255.0.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 1
Router(config-if)#redundancy group 1 ip 9.13.25.123 exclusive
Router(config-if)#h323-gateway voip interface
Router(config-if)#h323-gateway voip bind srcaddr 203.0.113.12

Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#ip address 192.0.2.1 255.255.255.0
Router(config-if)#media-type rj45
Router(config-if)#negotiation auto
Router(config-if)#redundancy rii 2
Router(config-if)#redundancy group 1 ip 192.0.2.3 exclusive
Router(config-if)#h323-gateway voip interface
Router(config-if)#h323-gateway voip bind srcaddr 192.0.2.3

```

Step 6 Configure the Punt Policing feature.

SIP packets towards the virtual IP address and physical IP address match different punt-cause codes. The punt-rate of the virtual IP address with a punt-cause of 60, is lower than the punt-rate of the physical IP address.

To ensure that the behaviour of the SIP packets towards virtual and physical IP address remains the same, you must increase the punt-rate of the virtual IP address by using the **platform punt-policer** command in global configuration mode.

Note For Cisco IOS XE Releases 16.6.7, 16.9.4, 16.11.1, 16.12.1, 17.1.1 and later releases, you do not need to increase the punt-rate.

Example:

```

Router(config)# platform punt-policer 60 40000

```

In the preceding example, the `punt-rate` of the virtual IP address (`punt-cause 60`) is increased from the default value of 2000 to 40000.

The following table provides details of the fields of the CLI.

Table 99: CLI Fields

Keyword	Description
<code>platform punt-policer</code>	Configures the Punt Policing feature.
<code>60</code>	<i>punt-cause</i> —Punt cause. Range is 1–107. Punt cause of the virtual interface is 60.
<code>40000</code>	<i>punt-rate</i> —Rate limit in packets per second. Range is 10–146484.

Note The default punt rate value of the virtual IP address and the physical IP address varies with the router platform.

Note The default and maximum setting are platform specific. Default value is optimal for most deployments. Change the rate only when suggested by Cisco Support.

Step 7 Configure the RG group under **voice service voip**. This enables Box-to-box CUBE HA.

Example:

```
Router#voice service voip
Router (conf-voi-serv) #redundancy-group 1
```

Step 8 Configure the Media Inactivity timer.

The Media Inactivity Timer enables the active and standby router pair to monitor and disconnect calls if no Real-Time Protocol (RTP) packets are received within a configurable time period.

For the SIP calls, the switched over calls are cleared with signaling (as signaling information is preserved for switched calls).

The Media Inactivity Timer releases TCP-based and H.323-based calls. This is used to guard against any hung sessions resulting from the failover when a normal call disconnect does not clear the call.

You must configure the same duration for the Media Inactivity Timer on both routers. The default value is 30 seconds for SIP calls. The sample configuration is as follows:

Example:

```
Router(config)#ip rtcp report interval 9000
Router(config)#gateway
Router(config-gateway)#media-inactivity-criteria all
Router(config-gateway)#timer receive-rtp 1200
Router(config-gateway)#timer receive-rtcp 5
```

SIP call legs are cleared once the RTCP timer expires.

Step 9 Reload the router.

Once all the preceding configurations are completed, you must save the configurations, and reload the router.

Example:


```
Router>enable
Router#relaod
```

Step 10 Configure the peer router.

Follow the preceding steps to configure the standby router. Make sure that you use the correct IP addresses.

Step 11 Point the attached devices to the CUBE Virtual IP (VIP) address.

The IP-PBX, Unified SIP Proxy, or service provider must route the calls to CUBE's Virtual IP address.

HA configuration does not handle SIP messages to the CUBE's physical IP addresses.

- a. Go to **System** menu, and choose **Service Parameters**. At the bottom of the Service Parameters, enable **Advanced**.
- b. Set the **Allow TCP KeepAlives for SIP** to False.
- c. After this setting is saved, restart the CallManager Services.

Configuration Example



Note Please note that IPv6 configuration for high availability is supported for Cisco IOS XE Dublin 17.12.1a and later releases.

Active Router:

```
voice service voip
  no ip address trusted authenticate
  allow-connections sip to sip
  redundancy-group 1
sip
  bind control source-interface GigabitEthernet0/0/1 ipv6-address 2001:10:1:20::14
  bind media source-interface GigabitEthernet0/0/1 ipv6-address 2001:10:1:20::14
!
redundancy
  application redundancy
  group 1
    name cube_b2b_ha_1
    priority 125 failover threshold 75
    timers delay 30 reload 60
    control GigabitEthernet0/0/1 protocol 1
    data GigabitEthernet0/0/1
    track 1 shutdown
  protocol 1
    name cube_b2b_ha_1
    authentication text sol_ha1
!
track 1 interface GigabitEthernet0/0/1 line-protocol
!
interface GigabitEthernet0/0/1
  ip address 10.1.20.14 255.255.255.0
  negotiation auto
  ipv6 address 2001:10:1:20::14/119
  no mop enabled
  no mop sysid
```

```

redundancy rii 102
redundancy group 1 ip 10.1.20.135 exclusive
redundancy group 1 ipv6 2001:10:1:20::135/119 exclusive
!
interface GigabitEthernet0/0/2
ip address 198.51.100.1 255.255.255.0
negotiation auto
no mop enabled
no mop sysid

```

Standby Router:

```

voice service voip
no ip address trusted authenticate
allow-connections sip to sip
redundancy-group 1
sip
  bind control source-interface GigabitEthernet0/0/1 ipv6-address 2001:10:1:20::14
  bind media source-interface GigabitEthernet0/0/1 ipv6-address 2001:10:1:20::14
!
redundancy
application redundancy
  group 1
    name cube_b2b_ha_1
    priority 100 failover threshold 75
    timers delay 30 reload 60
    control GigabitEthernet0/0/1 protocol 1
    data GigabitEthernet0/0/1
    track 1 shutdown
  protocol 1
    name cube_b2b_ha_1
    authentication text sol_ha1
!
track 1 interface GigabitEthernet0/0/1 line-protocol
!
interface GigabitEthernet0/0/1
ip address 10.1.20.115 255.255.255.0
ipv6 address 2001:10:1:20::115/119 255.255.255.0
negotiation auto
no mop enabled
no mop sysid
redundancy rii 102
redundancy group 1 ip 10.1.20.135 exclusive
redundancy group 1 ipv6 2001:10:1:20::135/119 exclusive
!
interface GigabitEthernet0/0/2
ip address 10.1.40.115 255.255.255.0
negotiation auto
no mop enabled
no mop sysid

```

Tips to Troubleshoot

Use the following show and debug commands to troubleshoot High Availability issues:

- **show redundancy application group all**
- **show redundancy application transport clients**
- **show redundancy client domain all | inc VOIP RG**
- **show voice high-availability summary**

- **show voip fpi stats**
- **debug voip rtp session**
- **debug voice high-availability all**
- **debug voip fpi all**
- **debug redundancy application group {config | faults | media | protocol | rii transport | vp}**



Note Do not turn on a large number of debugs on a system carrying high volume of active call traffic.



CHAPTER 69

DSP High Availability Support

- [DSP High Availability Support](#) , on page 803
- [Prerequisites for DSP High Availability](#), on page 804
- [Features Supported with DSP High Availability](#), on page 804
- [Restrictions for DSP High Availability](#), on page 804
- [Tips to Troubleshoot](#), on page 805
- [Configuration Examples for DSP HA](#), on page 805

DSP High Availability Support

Cisco Unified Border Element (CUBE) DSP High Availability support for SIP-to-SIP calls is added for Box-to-Box and Inbox configurations. Earlier, calls that required DSP resources were not checkpointed. As a result, both the media and signaling sessions were not preserved after switchover resulting in call failure.



Note DSP HA is supported only for SIP-to-SIP calls.

Feature Information

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 100: Feature Information for DSP HA Support on CUBE

Feature Name	Releases	Feature Information
DSP HA Support on CUBE	Baseline Fuctionality	Provides DSP High availability support for SIP-to-SIP calls on Box-to-Box and Inbox redundancies.

Prerequisites for DSP High Availability

- LTI Transcoding
- DSP HA is supported only on the following routers and its corresponding modules:
 - Cisco ISR G2 series (PVDM3)
 - Cisco ASR 1000 series (SPA-DSP)
 - Cisco ISR 4000 series (PVDM4)
 - Cisco Catalyst 8200 Edge series
 - Cisco Catalyst 8300 Edge series
- The same type and capacity DSP modules must be used in the Active and Standby CUBE devices (box-to-box)
- The DSP modules must be installed in the same slot and subslot in the Active and Standby CUBE devices (box-to-box)
- The Active and Standby CUBE devices must have the same DSPFARM configurations (box-to-box)

Features Supported with DSP High Availability

- Transcoding with Supplementary Services
- Voice Class Codec
- G.711 in-band -> RFC2833 (RTP-NTE) DTMF interworking variant
- SRTP-RTP Interworking (ISR-G2 only)
- Fax calls with transcoder invoked for codec mis-match

Restrictions for DSP High Availability

- Media flow-around calls are not supported.
- SDP passthrough calls are not supported.
- Audio Transrating is not supported.
- Call Progress Analysis is not supported.
- Dolby Noise Reduction (NR) and Acoustic Shock Protection (ASP) are not supported.
- All SCCP-based media resources (Conference bridge, Transcoding, HW MTP, and SW MTP) are not supported with Cisco Unified Border Element High Availability.

Tips to Troubleshoot

You can use the following debug commands to troubleshoot DSP HA:

- debug voip dsmp all
- debug voip dsm all
- debug ccscip message
- debug voip ipipgw
- debug voip ipipgw high-availability
- debug voip high-availability all
- debug media resource provisioning all
- debug dsp-resource-manager flex dspfarm
- debug dsp-resource-manager flex function
- debug dsp-resource-manager flex error

Configuration Examples for DSP HA

Active Configuration

```
-----  
voice-card 0  
  dsp services dspfarm  
  
dspfarm profile 2 transcode universal  
  codec g711ulaw  
  codec g711alaw  
  codec g729ar8  
  codec g729abr8  
  maximum sessions 100  
  associate application CUBE
```

Standby Configuration

```
-----  
voice-card 0  
  dsp services dspfarm  
  
dspfarm profile 2 transcode universal  
  codec g711ulaw  
  codec g711alaw  
  codec g729ar8  
  codec g729abr8  
  maximum sessions 100  
  associate application CUBE
```

The following example shows the DSP HA output for the active and standby configurations:

On Active:

```
Mang-Active#show dspfarm dsp active
SLOT  DSP VERSION  STATUS CHNL USE  TYPE  RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED
0      13      39.0.0      UP      1      USED  xcode      1      16558
      3005      3007
0      13      39.0.0      UP      1      USED  xcode      1      16559
      3004      3005
```

Total number of DSPFARM DSP channel(s) 1

On Standby:

```
Mang-Standby#show dspfarm dsp active
SLOT  DSP VERSION  STATUS CHNL USE  TYPE  RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED
0      13      39.0.0      UP      1      USED  xcode      1      16558
      0      0
0      13      39.0.0      UP      1      USED  xcode      1      16559
      0      0
```

Total number of DSPFARM DSP channel(s) 1



CHAPTER 70

Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices

- [Overview, on page 807](#)
- [Prerequisites for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices, on page 810](#)
- [Restrictions for Stateful Switchover Between Redundancy Paired Intra- or Inter-box Devices, on page 811](#)
- [High Availability Protected Mode and Box-to-Box Redundancy for ASR, on page 811](#)
- [Support for Box-to-Box High Availability with Virtual IP Addresses, on page 812](#)
- [Monitor Call Escalation and De-escalation with Stateful Switchover, on page 812](#)
- [Monitor Media Forking with High Availability, on page 814](#)
- [Verify the High Availability Protected Mode, on page 816](#)
- [Support for REFER and BYE/Also after Stateful Switch-Over, on page 817](#)
- [Tips to Troubleshoot, on page 818](#)
- [Example: Configuring SIP Binding, on page 819](#)

Overview

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.

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.
- 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*.

Feature Information

Table 101: Feature Information

Feature Name	Releases	Feature Information
Stateful Switchover Between Redundancy Paired Intra or Inter-box Devices	Baseline Functionality	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.

Call Escalation with Stateful Switchover

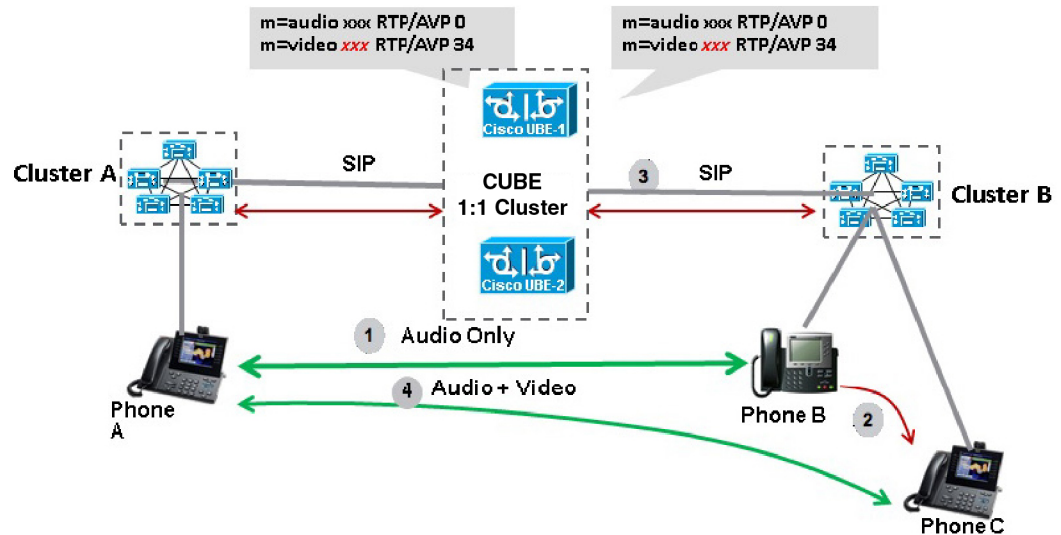
The call escalation workflow is as follows:

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 (CUBE).
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 CUBE switchover happens at any instance, then audio calls will be preserved before escalation and video calls will be preserved after escalation.

Figure 73: Call Escalation



336002

Call De-escalation with Stateful Switchover

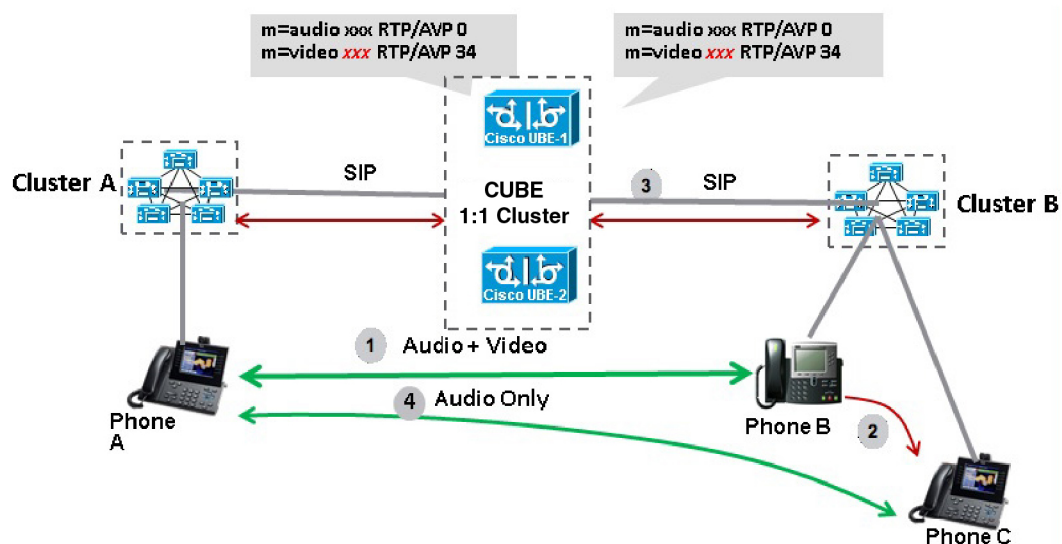
The call de-escalation workflow is as follows:

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 (CUBE).
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 CUBE switchover happens at any instance, then video calls will be preserved before de-escalation and audio calls will be preserved after de-escalation.

Figure 74: Call De-escalation



336003

Media Forking with High Availability

Media forking with high availability is supported on ISR G2, ISR G3 and ASR platforms. When a primary call is connected and a forked call-leg is established on an active CUBE device, both the primary and the forked call-leg will be checkpointed in the standby CUBE 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 CUBE” module in the [CUBE Protocol-Independent Features and Setup Configuration Guide](#).

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

- Call escalation and de-escalation are not supported in REFER consumption mode.
- Session Description Protocol (SDP) passthru calls are not supported.
- Resource Reservation Protocol (RSVP) is not supported.
- Alternative Network Address Types (ANAT) for IPv4 or IPv6 interworking is not supported.
- 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.

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.
- In a high availability scenario, if CUBE in standby redundancy group (RG) state is already in VoIP HA protected mode and a switchover occurs, causing the standby CUBE to become active on RG level, VoIP functionality is disabled. This is because incoming call processing is disabled in VoIP HA protected mode, so even when the standby CUBE assumes the active role on RG level, call processing remains

impaired. The only way to restore call processing is to manually reboot the affected CUBE instance to exit protected mode.

To enable 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.

Example: Configuring the Interfaces for ASR Devices

ASR (RG Infra-based)

```
interface GigabitEthernet0/0/0
 ip address 10.13.25.190 255.255.0.0
 negotiation auto
 redundancy rii 1
 redundancy group 1 ip 10.13.25.123 exclusive
```

Support for Box-to-Box High Availability with Virtual IP Addresses

The OPTIONS ping with CUBE high availability feature adds the ability to match the incoming dial-peer in the context of the OPTIONS message, allowing response with the virtual IP address shared between the active and standby CUBEs. Box-to-box high availability is supported using virtual IP addresses for the signaling and media, by enhancing the CUBE response to an inbound OPTIONS ping message. This is possible because dial-peer matching of a request URI that does not have a user part is supported.



Important

When OPTIONS Ping SIP Trunk (from CUCM) is configured to CUBE that is running in HA mode, the SIP Trunk goes down whenever the active interface goes down. The SIP Trunk comes back in service, when the OPTIONS Ping next retry happens to CUBE HA node. The default retry time is 60 seconds.



Note

For configuration examples, see the Examples section about configuring interfaces (ISR and ASR) and configuring SIP binding.

Monitor 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 CUBE 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
```

Monitor Media Forking with High Availability

Perform this task to monitor media forking calls with high availability on active and standby CUBE 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 CUBE 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
```

```
REC MSP 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 src 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 src 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

```

Verify 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-availability rf-client** (active device)
3. **show voice high-availability rf-client** (standby device)

DETAILED STEPS

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

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

Example:

```
Device# show voice high-availability 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-availability rf-client** (standby device)

Example:

```
Device# show voice high-availability 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)]

```

Support for REFER and BYE/Also after Stateful Switch-Over

REFER based supplementary services with high availability is supported post-stateful switchover on CUBE. Support is also provided for SIP-to-SIP BYE/Also calls.

Use the **show sip-ua handoff stats** command to display the call handoff statistics for calls handed off successfully after switchover. Following are the statistics displayed:

- Total number of calls handed off
- Total number of successful calls handoffs
- Total numbers of unsuccessful call handoffs

The following sample output displays the call handoff statistics:

```
2951-CUBE#show sip-ua handoff stats
Total Calls Handed Off      = 1
Successful Call Hand offs   = 1
Un-Successful Call Hand offs = 0
2951-CUBE#
```

Tips to Troubleshoot

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**

Use the following debug commands to troubleshoot issues related to handling of REFER based supplementary services:

- **debug ccsip verbose**
- **debug voip application all**
- **debug voip ccapi all**
- **debug voice high-availability all**

Example: Configuring SIP Binding

```
dial-peer voice inbound-dial-peer-tag voip
  session protocol sipv2
  incoming uri from mydesturi
  voice-class sip call-route url
  voice-class sip bind control source-interface GigabitEthernet 0/0/0
!
voice class uri mydesturi
  host abc.com
```




CHAPTER 71

CVP Survivability TCL support with High Availability

- [Overview, on page 821](#)
- [Prerequisites, on page 822](#)
- [Restrictions, on page 822](#)
- [Recommendations, on page 822](#)
- [Configure CVP Survivability TCL support with High Availability, on page 822](#)

Overview

Call survivability features are supported in Cisco Unified Border Element (CUBE) high availability mode for all active calls handled by Cisco Voice Portal (CVP).

Contact Center Deployments use call survivability TCL script on CUBE to provide basic Call survivability services when downstream CVP nodes are not reachable. From Cisco IOS Release 15.6(2)T onwards, call survivability features are supported in CUBE High Availability mode. Post switchover, all events received on the calls handled by CVP are posted to Call Survivability TCL application for further processing. Thus, call survivability features are supported in CUBE high availability mode for all active calls handled by CVP.

For more information on CVP Call Survivability TCL, refer to http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp9_0/configuration/guide/cvp-configuration-and-administration-guide.pdf

Feature Information

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 102: Feature Information for CVP Survivability TCL support with High Availability

Feature Name	Releases	Feature Information
CVP Survivability TCL support with High Availability	Baseline Functionality	This feature enables CUBE support call survivability features in CUBE high availability mode for all active calls handled by CVP.

Prerequisites

CVP survivability TCL application is configured on incoming dial-peer.

Restrictions

- If there is a courtesy callback (CCB) registered with CVP, then post switchover, CCB is not supported.
- Only call survivability TCL script is supported with CUBE high availability. Other TCL based services are not supported.
- Only the active calls will be check pointed. (Calls which are connected - 200OK / ACK transaction completed). Calls in transition state will not be check pointed.

Recommendations

Configure TCP session transport for the SIP trunk between CUBE and CVP.

Configure CVP Survivability TCL support with High Availability

Existing configuration of applying the survivability TCL application on incoming dial-peer is sufficient. No additional configuration required.



PART **XII**

Cloud Services

- [Hosted Scenarios \(Lineside Connectivity\), on page 825](#)
- [Configure SIP Registration, on page 827](#)
- [Survivability Enhancements, on page 843](#)
- [SUBSCRIBE-NOTIFY Passthrough, on page 863](#)



CHAPTER 72

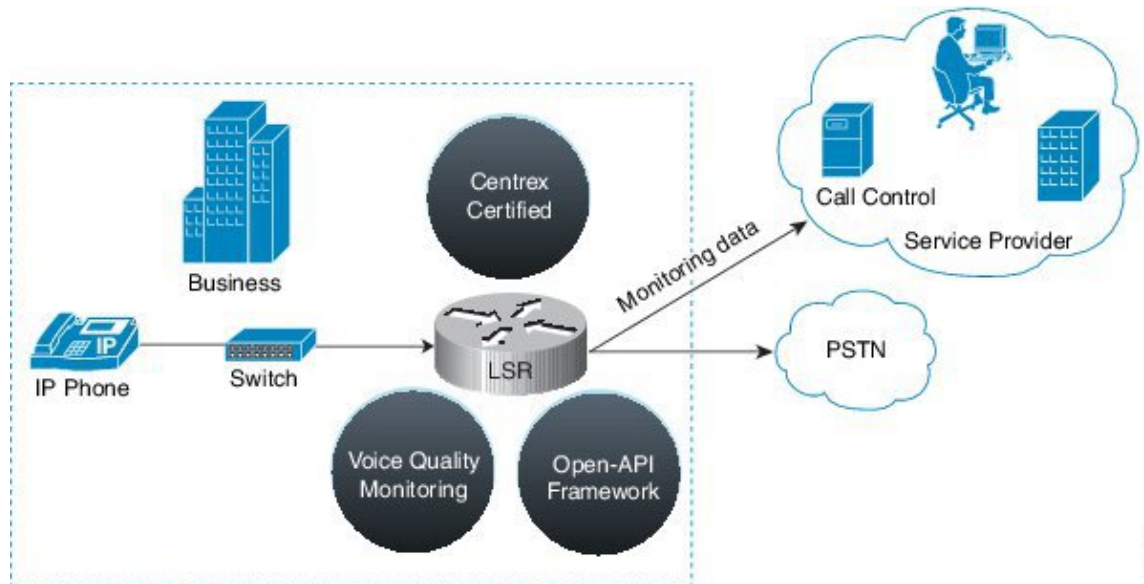
Hosted Scenarios (Lineside Connectivity)

- [Hosted and Cloud Services Delivery, on page 825](#)

Hosted and Cloud Services Delivery

CUBE delivers hosted and cloud based communication services at customer sites by managing registration traffic and ensuring uninterrupted service, when the remote call control platform becomes unreachable.

Figure 75: CUBE in Hosted and Cloud Services



384137



CHAPTER 73

Configure SIP Registration

- [Overview, on page 827](#)
- [Prerequisites, on page 832](#)
- [Restrictions, on page 832](#)
- [Configure SIP Registration Proxy, on page 832](#)
- [Configuration Example-Hosted and Cloud Services SIP Registration Proxy, on page 841](#)

Overview

The Cisco Unified Border Element (CUBE) SIP Registration Proxy feature allows service providers to control the flow of registration messages between a customer's private network and their hosted communications platform.

By controlling routine registration traffic at the customer site, service providers can ensure service availability to local endpoints, while protecting core services from high message loads.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.

Feature Information for SIP Registration Proxy

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 103: Feature Information for Support for SIP Registration Proxy on CUBE

Feature Name	Releases	Feature Information
Support for CUBE SIP Registration Proxy	Cisco IOS XE Fuji 16.9.1	<p>CUBE SIP Registration Proxy supports sending outbound registrations from CUBE based on incoming registrations. This feature enables direct registration of SIP endpoints with the SIP registrar in hosted Unified Communications deployments. This feature also provides various benefits for handling CUBE deployments with no IPPBX support.</p> <p>The following commands were introduced or modified: authentication (dial peer), registrar server, registration passthrough, registration spike, show sip-ua registration passthrough status, voice-class sip registration passthrough static rate-limit.</p>

Registration Pass-Through Modes

CUBE uses the following two modes for registration pass-through:

End-to-End Mode

In the end-to-end mode, Cisco Unified Border Element (CUBE) collects the registrar details from the Uniform Resource Identifier (URI) and passes the registration messages to the registrar. The registration information contains the expiry time for rate-limiting, the challenge information from the registrar, and the challenge response from the user.

CUBE also passes the challenge to the user if the register request is challenged by the registrar. The registrar sends the 401 or 407 message to the user requesting for user credentials. This process is known as challenge.

CUBE ignores the local registrar and authentication configuration in the end-to-end mode. It passes the authorization headers to the registrar without the header configuration.

End-to-End Mode--Call Flows

This section explains the following end-to-end pass-through mode call flows:

Register Success Scenario

The successful register scenario for the end-to end registration pass-through mode is as follows:

1. The user sends the register request to CUBE.
2. CUBE matches the request with a dial peer and forwards the request to the registrar.
3. CUBE receives a success response message (200 OK message) from the registrar and forwards the message to the endpoint (user).
4. The registrar details and expiry value are passed to the user.

Registrar Challenging the Register Request Scenario

The following scenario explains how the registrar challenges the register request:

1. The user sends the register request to CUBE.
2. CUBE matches the register request with a dial peer and forwards it to the registrar.
3. The registrar challenges the register request.
4. CUBE passes the registrar response and the challenge request, only if the registrar challenges the request to the user.
5. The user sends the register request and the challenge response to the CUBE.
6. CUBE forwards the response to the registrar.
7. CUBE receives success message (200 OK message) from the registrar and forwards it to the user.

Peer-to-Peer Mode

In the peer-to-peer registration pass-through mode, the outgoing register request uses the registrar details from the local CUBE configuration. CUBE answers the challenges received from the registrar using the configurable authentication information. CUBE can also challenge the incoming register requests and authenticate the requests before forwarding them to the network.

In this mode, CUBE sends a register request to the registrar and also handles register request challenges. That is, if the registration request is challenged by the registrar (registrar sends 401 or 407 message), CUBE forwards the challenge to the user and then passes the challenge response sent by the user to the registrar. In the peer-to-peer mode, CUBE can use the **authentication** command to calculate the authorization header and then challenge the user depending on the configuration.



Note The **registrar** command must be configured in peer-to-peer mode. Otherwise, the register request is rejected with the 503 response message.

Peer-to-Peer Mode--Call Flows

This section explains the following peer-to-peer pass-through mode call flows:

Register Success Scenario

The register success scenario for a peer-to-peer registration pass-through mode is as follows:

1. The user sends the register request to CUBE.
2. CUBE matches the register request with a dial peer and forwards the register request to the registrar.
3. CUBE receives a success message (200 OK message) from the registrar and forwards it to the endpoint (user). The following functions are performed:
 - CUBE picks up the details about the registrar from the configuration.
 - CUBE passes the registrar details and expiry value to the user.

Registrar Challenging the Register Request Scenario

The following scenario explains how the registrar challenges the register request:

1. The user sends the register request to CUBE.
2. CUBE matches the register request with a dial peer and forwards the register request to the registrar.
3. The user responds to the challenge request.
4. CUBE validates the challenge response and forwards the register request to the registrar.
5. CUBE receives a success message from the registrar and forwards it to the endpoint (user).

Registration in Different Registrar Modes

This section explains SIP registration pass-through in the following registrar modes:

Primary-Secondary Mode

In the primary-secondary mode the register message is sent to both the primary and the secondary registrar servers simultaneously.

The register message is processed as follows:

- The first successful response is passed to the phone as a SUCCESS message.
- All challenges to the request are handled by CUBE.
- If the final response received from the primary and the secondary servers is an error response, the error response that arrives later from the primary or the secondary server is passed to the phone.
- If only one registrar is configured, a direct mapping is performed between the primary and the secondary server.
- If no registrar is configured, or if there is a Domain Name System (DNS) failure, the "503 service not available" message is sent to the phone.

DHCP Mode

In the DHCP mode the register message is sent to the registrar server using DHCP.

Multiple Register Mode

In the multiple register mode, you can configure a dial peer to select and enable the indexed registrars. Register messages must be sent only to the specified index registrars.

The response from the registrar is mapped the same way as in the primary-secondary mode.

Registration Overload Protection

The registration overload protection functionality enables CUBE to reject the registration requests that exceed the configured threshold value.

To support the registration overload protection functionality, CUBE maintains a global counter to count all the pending outgoing registrations and prevents the overload of the registration requests as follows:

- The registration count is decremented if the registration transaction is terminated.
- The outgoing registrations are rejected if the count goes beyond a configured threshold.

- The incoming register request is rejected with the 503 response if the outgoing registration is activated by the incoming register request.
- A retry timer set for a random value is used for attempting the registration again if the registrations are originated from CUBE.

The registration overload protection functionality protects the network from the following:

- Avalanche Restart-All the devices in the network restart at the same time.
- Component Failures-Sudden burst of load is routed through the device due to a device failure.

Registration Overload Protection-Call Flow

The following steps explain the register overload protection scenario:

1. The user sends a register request to CUBE.
2. CUBE matches the request with a dial peer and forwards the register request to the registrar.
3. The registration is rejected with a random retry value when the registration threshold value is reached.



Note The call flow for the DNS query on the Out Leg is the same for the end-to-end and peer-to-peer mode.

Registration Rate-limiting

The registration rate-limiting functionality enables you to configure different SIP registration pass-through rate-limiting options. The rate-limiting options include setting the expiry time and the fail count value for a Cisco UBE. You can configure the expiry time to reduce the load on the registrar and the network. CUBE limits the reregistration rate by maintaining two different timers--in-registration timer and out-registration timer.

The initial registration is triggered based on the incoming register request. The expiry value for the outgoing register is selected based on the CUBE configuration. On receiving the 200 OK message (response to the BYE message) from the registrar, a timer is started using the expiry value available in the 200 OK message. The timer value in the 200 OK message is called the out-registration timer. The success response is forwarded to the user. The expiry value is taken from the register request and the timer is started accordingly. This timer is called the in-registration timer. There must be a significant difference between the in-registration timer and the out-registration timer values for effective rate-limiting.

Registration Rate-limiting Success--Call Flow

The following steps explain a scenario where the rate-limiting functionality is successful:

1. The user sends the register request to CUBE.
2. CUBE matches the registration request with a dial peer and forwards it to the registrar. The outgoing register request contains the maximum expiry value if the rate-limiting functionality is configured.
3. The registrar accepts the registration.
4. CUBE forwards the success response with the proposed expiry timer value.

5. The user sends the reregistration requests based on the negotiated value. CUBE resends the register requests until the out-leg expiry timer value is sent.
6. CUBE forwards the subsequent register request to the registrar, if the reregister request is received after the out-leg timer is reached.

Prerequisites

- You must enable the local SIP registrar. See [Enable Local SIP Registrar, on page 832](#) .
- You must configure dial peers manually for call routing and pattern matching

Restrictions

Does not support IPv6.

Configure SIP Registration Proxy

Enable Local SIP Registrar

Perform this task to enable the local SIP registrar.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **registrar server** [**expires** [**max value**] [**min value**]]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters voice-service configuration mode.
Step 4	sip Example: <pre>Device(conf-voi-serv)# sip</pre>	Enters service SIP configuration mode.
Step 5	registrar server [expires [max value] [min value]] Example: <pre>Device(conf-serv-sip)# registrar server</pre>	<p>Enables the local SIP registrar.</p> <ul style="list-style-type: none"> • Optionally you can configure the expiry time of the registrar using the following keywords: <ul style="list-style-type: none"> • expires--Configures the registration expiry time. • max--Configures the maximum registration expiry time. • min--Configures the minimum registration expiry time. <p>Note The registrar command must be configured in peer-to-peer mode. Otherwise, the register request is rejected with the 503 response message.</p>
Step 6	end Example: <pre>Device(conf-serv-sip)# end</pre>	Exits service SIP configuration mode and returns to privileged EXEC mode.

Configure SIP Registration Proxy at the Global Level

Perform this task to configure SIP registration proxy at the global level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **registration passthrough [system | [static | dynamic [local-fallback value]] [rate-limit [expires value] [fail-count value]] [reg-sync value] [registrar-index index]]**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters voice-service configuration mode.
Step 4	sip Example: <pre>Device(conf-voi-serv)# sip</pre>	Enters service SIP configuration mode.
Step 5	registration passthrough [system [static dynamic [local-fallback <i>value</i>]] [rate-limit [expires <i>value</i>] [fail-count <i>value</i>]] [reg-sync <i>value</i>] [registrar-index <i>index</i>]] Example: <pre>Device(conf-serv-sip)# registration passthrough</pre>	Configures the SIP registration pass-through options. <ul style="list-style-type: none"> • You can specify different SIP registration pass-through options using the following keywords: <ul style="list-style-type: none"> • dynamic—SIP Registration uses the dynamic registrar details (default). • local-fallback—Configures Local Fallback - (e2e). • rate-limit—Enables rate-limiting. • reg-sync—Sends REGISTER messages when registrar up (p2p). • registrar-index—Configures a list of registrars to be used for registration. For detailed information, see Configuring Multiple Registrars on SIP Trunks. • static—SIP Registration Use static Registrar Details. • system—Use system registration passthrough configuration.
Step 6	end Example:	Exits service SIP configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(conf-serv-sip)# end	

Configure SIP Registration Proxy at the Tenant Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class tenant tag**
4. **registrar { dhcp | [registrar index] registrar-server-address [:port] | expires value }**
5. **registration passthrough [system | [static | dynamic [local-fallback value]] [rate-limit [expires value] [fail-count value]] [reg-sync value] [registrar-index index]]**
6. **exit**
7. **dial-peer voice tag voip**
8. **voice-class sip tenant tag**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class tenant tag Example: Device(config)# voice class tenant 1	Enters the tenant configuration mode.
Step 4	registrar { dhcp [registrar index] registrar-server-address [:port] expires value } Example: Device(config-class)#registrar ipv4:10.65.75.45:9052 expires 3600	Configures the registrar server.
Step 5	registration passthrough [system [static dynamic [local-fallback value]] [rate-limit [expires value] [fail-count value]] [reg-sync value] [registrar-index index]]	Configures SIP registration pass-through options on a dial peer on a dial peer.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(config-class)# registration passthrough static</pre>	<ul style="list-style-type: none"> You can specify different SIP registration pass-through options using the following keywords: <ul style="list-style-type: none"> dynamic—SIP Registration uses the dynamic registrar details (default). local-fallback—Configures Local Fallback - (e2e). rate-limit—Enables rate-limiting. reg-sync—Sends REGISTER messages when registrar up (p2p). registrar-index—Configures a list of registrars to be used for registration. For detailed information, see Configuring Multiple Registrars on SIP Trunks. static—SIP Registration Use static Registrar Details. system—Use system registration passthrough configuration.
Step 6	<p>exit</p> <p>Example:</p> <pre>Device(config-class)# exit</pre>	Exits tenant configuration mode and returns to global configuration mode.
Step 7	<p>dial-peer voice tag voip</p> <p>Example:</p> <pre>Device(config)# dial-peer voice 444 voip</pre>	Enters dial peer voice configuration mode.
Step 8	<p>voice-class sip tenant tag</p> <p>Example:</p> <pre>Device(config-dial-peer)# voice-class sip tenant 1</pre>	Associates the dial-peer with the tenant.
Step 9	<p>exit</p> <p>Example:</p> <pre>Device(config-class)# exit</pre>	Exits dial-peer configuration mode and returns to global configuration mode.

Configure SIP Registration Proxy at the Dial Peer Level

Perform this task to configure SIP registration proxy at the dial peer level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip registration passthrough [system | [static | dynamic [local-fallback value]] [rate-limit [expires value] [fail-count value]] [reg-sync value] [registrar-index index]]**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: <pre>Device(config)# dial-peer voice 444 voip</pre>	Enters dial peer voice configuration mode.
Step 4	voice-class sip registration passthrough [system [static dynamic [local-fallback value]] [rate-limit [expires value] [fail-count value]] [reg-sync value] [registrar-index index]] Example: <pre>Device(config-dial-peer)# voice-class sip registration passthrough static</pre>	Configures SIP registration pass-through options on a dial peer on a dial peer. <ul style="list-style-type: none"> • You can specify different SIP registration pass-through options using the following keywords: <ul style="list-style-type: none"> • dynamic—SIP Registration uses the dynamic registrar details (default). • local-fallback—Configures Local Fallback - (e2e). • rate-limit—Enables rate-limiting. • reg-sync—Sends REGISTER messages when registrar up (p2p). • registrar-index—Configures a list of registrars to be used for registration. For detailed information, see Configuring Multiple Registrars on SIP Trunks. • static—SIP Registration Use static Registrar Details.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • system—Use system registration passthrough configuration.
Step 5	exit Example: Device(config-dial-peer)# exit	Exits dial peer voice configuration mode and returns to global configuration mode.

Configure Registration Overload Protection

Perform this task to configure registration overload protection functionality on CUBE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **registration spike** *max-number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	sip-ua Example: Device(config)# sip-ua	Enters SIP user-agent configuration mode.
Step 4	registration spike <i>max-number</i> Example: Device(config-sip-ua)# registration spike 100	Configures registration overload protection functionality on CUBE.
Step 5	end Example:	Exits SIP user-agent configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-sip-ua)# end	

Configure CUBE to Route a Call to the Registrar Endpoint

Perform this task to configure CUBE to route a call to the registrar endpoint.



Note You must perform this configuration on a dial peer that is pointing towards the endpoint.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag {pots | voatm | vofr | voip}
4. session target registrar
5. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	dial-peer voice tag {pots voatm vofr voip} Example: Device(config)# dial-peer voice 444 voip	Enters dial peer voice configuration mode.
Step 4	session target registrar Example: Device(config-dial-peer)# session target registrar	Configures CUBE to route the call to the registrar endpoint.
Step 5	exit Example: Device(config-dial-peer)# exit	Exits dial peer voice configuration mode and returns to global configuration mode.

Verify the SIP Registration

Perform this task to verify the configuration for SIP registration on CUBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show sip-ua registration passthrough status**
3. **show sip-ua registration passthrough status detail**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show sip-ua registration passthrough status**

Displays the SIP user agent (UA) registration pass-through status information.

Example:

```
Device# show sip-ua registration passthrough status
```

```
CallId      Line          peer          mode In-Exp      reg-I Out-Exp
=====
771         5500550055   1             p2p  64          1     64
=====
```

Step 3 **show sip-ua registration passthrough status detail**

Displays the SIP UA registration pass-through status information in detail.

Example:

```
Device# show sip-ua registration passthrough status detail
```

```
=====
Configured Reg Spike Value: 0
Number of Pending Registrations: 0
=====
Call-Id: 763
Registering Number: 5500550055
Dial-peer tag: 601
Pass-through Mode: p2p
Negotiated In-Expires: 64 Seconds
Next In-Register Due in: 59 Seconds
In-Register Contact: 9.45.36.5
-----
Registrar Index: 1
Registrar URL: ipv4:9.45.36.4
Negotiated Out-Expires: 64 Seconds
Next Out-Register After: 0 Seconds
=====
```

The following section will be added to the "Examples" section of the SIP to SIP chapter.

Configuration Example-Hosted and Cloud Services SIP Registration Proxy

```
!
!
voice service voip
sip
    registrar server expires max 121 min 61
    registration passthrough static rate-limit expires 9000 fail-count 5 registrar-index 1 3
    5
!
dial-peer voice 1111 voip
destination-pattern 1234
voice-class sip pass-thru content unsupp
session protocol sipv2
session target registrar
!
dial-peer voice 1111 voip
destination-pattern 1234
voice-class sip pass-thru content unsupp
voice-class sip registration passthrough static rate-limit expires 9000 fail-count 5
registrar-index 1 3 5
authentication username 1234 password 7 075E731F1A realm cisco.com
session protocol sipv2
session target registrar
!
sip-ua
registration spike 1000
!
!
```




CHAPTER 74

Survivability Enhancements

- [Overview](#) , on page 843
- [Configure Survivability for Hosted and Cloud Services](#), on page 848
- [Verify Survivability](#), on page 858
- [Configuration Examples—Survivability for Hosted and Cloud Services](#) , on page 860

Overview

The Survivability for Hosted and Cloud Services on the CUBE is used to:

- Monitor the WAN status periodically from the CUBE.
- Route calls and handle line-side subscriptions locally when the WAN link is down.
- Synchronize the registrations with the server when the WAN link is up.

Advantages of Using CUBE Survivability Feature

The survivability feature on CUBE addresses the following issues by providing local fallback or registration synchronization:

1. When a WAN link or registrar server comes up, it waits until each SIP phone sends the REGISTER message to the server, so that outside phones can reach that phone.
2. If the phone register timer setting is too large, the outside phone waits that much time to reach that phone, after a link flap.
3. If the phone register timer setting is too small, it floods the WAN link.
4. When the WAN link or registrar server is down, you cannot make any local calls.

Local Fallback

- CUBE does not need to configure credentials, as the phones trigger registration. Although CUBE receives REGISTER messages for each phone every 5 minutes; for example, it throttles and sends REGISTER messages every 1 hour to the registrar server, avoiding high WAN bandwidth usage. This addresses the issues 1, 2, and 3.

- In normal operation when the WAN link or registrar server is up, the phone's primary server URL is the registrar server (E2E) registration.
- "OPTIONS ping" is used to monitor the registrar server link status. When the detected link is down, CUBE replies with a 500 message and when the phone receives this message, it sends the REGISTER message to CUBE, which is the secondary server (P2P registration). CUBE replies with a 200 OK message to P2P registration when the link is down. The dial-peer keeps the dynamic registrar session target and the local call does not fail. This addresses issue 4.

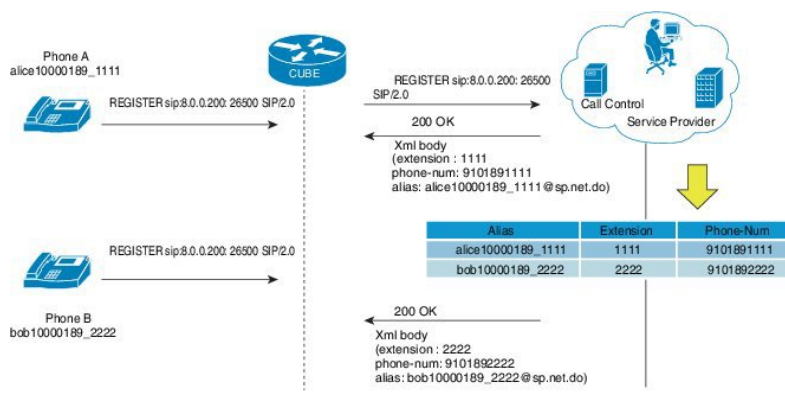
Registration Synchronization

- If you configure the phones to send REGISTER messages every 1 hour (to help alleviate the WAN link), the CUBE uses the credentials that were configured to respond to registrar server authentication challenge. This addresses issue 3.
- When the WAN link or registration server is down (detected by OPTIONS ping), the CUBE keeps the registration database of the SIP phones that were previously registered successfully, and it does not send REGISTER messages out; CUBE replies with a 200 OK message and dial-peer keeps the dynamic registrar session target. The local call does not fail, addressing issue 4.
- When the registrar link is up after a link flap, the CUBE sends REGISTER message for each phone that was earlier successfully registered to the registrar server. This is throttled to avoid bulk REGISTER messages flooding WAN link and the registrar. This addresses issues 1 and 2.

Registration Through Alias Mapping

The following illustration shows how a phone (with alias mapping) registers to the service provider through CUBE.

Figure 76: SIP Phone Registration



The addresses-of-record (AOR) sent in the REGISTER is an alias which is mapped to an extension and (or) phone number by the service provider. The service provider returns the mapping details in the 200 OK response sent to the REGISTER. CUBE has the ability to cache the alias mapping details in its call routing database. When a call is made from the phone, the Request-URI of the INVITE contains the dialed number (short extension or phone number).

If WAN is up, CUBE always routes the INVITE sent from the phone to the service provider without looking up at the alias mapping cache.

If WAN or the service provider is down, that is, in survivability mode, CUBE routes the INVITE locally by looking up at the alias mapping cache.

Alias Mapping—Supported Methods

1. When the service provider returns the mapping details in the 200 OK message of the REGISTER in the following predefined format:

Alias	Extension	Phone
alice10000189_1111	1111	10000189

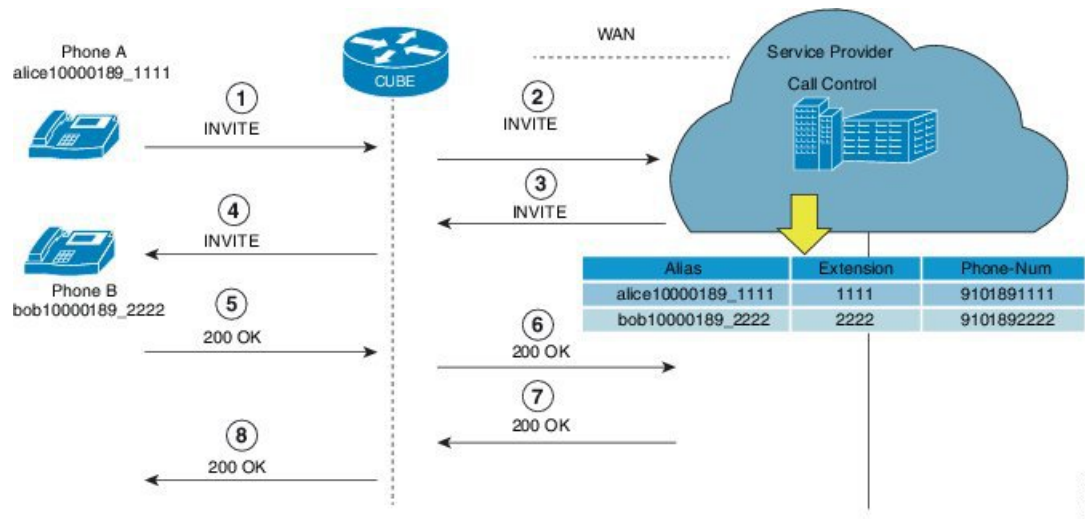
2. The short extension or phone number is embedded in the AOR of the REGISTER. For example, AOR is **alice10000189_1111** and the short extension is **1111**.

An inbound sip profile can be applied to the REGISTER which extracts the extension part from the AOR and adds an X-CISCO-EXTENSION header.

CUBE Survivability When WAN is UP

The following illustration provides an example as to how a typical phone makes a call to another local phone registered in the same server when WAN or the registrar server is up in a typical hosted deployment. The circled numbers in the image indicate the numerical order in which the sequence occurs.

Figure 77: WAN Link is UP - CUBE Deployment



The call flow scenario is as follows: Phone A initiates a call to the Phone B registered to the same server.

1. Phone A sends an initial INVITE request to Phone B to participate in a call session through CUBE.
2. CUBE sends this INVITE to the service provider.
3. The service provider in turn sends the INVITE to CUBE. Since the WAN link is up, the service provider maps details of the user from the register server and provides details of the user, for example, alias of the user, short extension number, and phone number.
4. CUBE sends INVITE with all the above mentioned information to Phone B.

Example: Normal Mode (WAN is Up in P2P Mode)

5. Phone B sends a 200 OK response to CUBE for the received INVITE.
6. CUBE sends a 200 OK answer to the service provider.
7. The service provider responds to CUBE with a 200 OK answer.
8. A final 200 OK response is sent to Phone A by CUBE and the call is established between Phone A and Phone B.

Example: Normal Mode (WAN is Up in P2P Mode)

```
CUBE# show sip-ua registration passthrough status
```

CallId	DirectoryNum	peer	mode	In-Exp	reg-I	Out-Exp	survival
21	NCPPhone1006	1	p2p	135 /144	1	144	normal

Example: Normal Mode (WAN is Up in E2E Mode)

```
CUBE# show sip-ua registration passthrough status
```

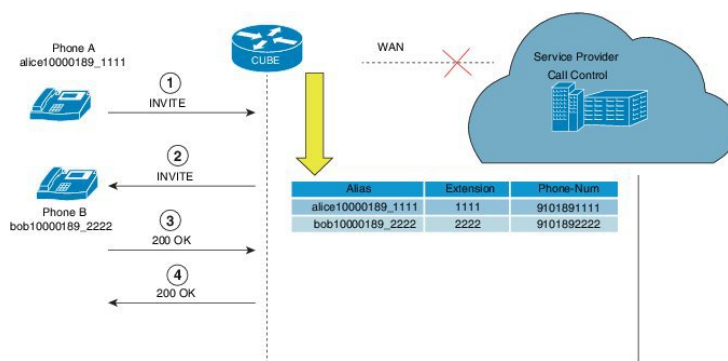
CallId	DirectoryNum	peer	mode	In-Exp	reg-I	Out-Exp	survival
14574	NCPPhone1006	301	e2e	117 /120	--	120	normal

CUBE Survivability When WAN Is Down

In survivability mode, CUBE provides end-to end telephony services when access to the centralized servers is interrupted because of a WAN outage or other factors, like the server being down.

The following illustration shows how a call is established between two endpoints when WAN link is down during survivability by directly dialing into an extension.

Figure 78: CUBE Survivability When WAN Is Down



Earlier, when WAN was down, User A could only contact User B using either the alias or the user-id of User B, and not using their extensions or phone numbers.

Now, in the event the WAN link or registration server is down, when a local call is made, INVITE is sent to CUBE. CUBE maps the details of the user like the extension number and phone-number stored during registration. Local phones can now be reached on their short extensions or phone numbers by similar phones that are subscribed to the server through the same CUBE.

It is possible to register multiple contacts for a single AOR; however, if multiple contacts are registered for a single subscriber, the CUBE uses only the topmost registered contact to deliver the call to that subscriber. For this reason, multiple contacts are not supported.

A few phone models, such as, Cisco IP Phone 7800 Series with Multiplatform Firmware and Cisco IP Phone 8800 Series with Multiplatform Firmware, sends register request to primary registrar only and do not send secondary REGISTER request to the secondary registrar (CUBE) in E2E mode when primary registrar could not be reached. In such scenarios, phone service goes down after it receives 500 response from CUBE for REGISTER request toward primary registrar.

To avoid phones getting into such error condition, CUBE checks for the response from the primary registrar side. When CUBE receives request timeout on WAN side or responses other than 200, 4XX, and 3XX from primary registrar, survivability will be enabled.

To enable survivability on such phones, refer [Configuring Survivability for Phones Sending Single Register Request](#), on page 851 .

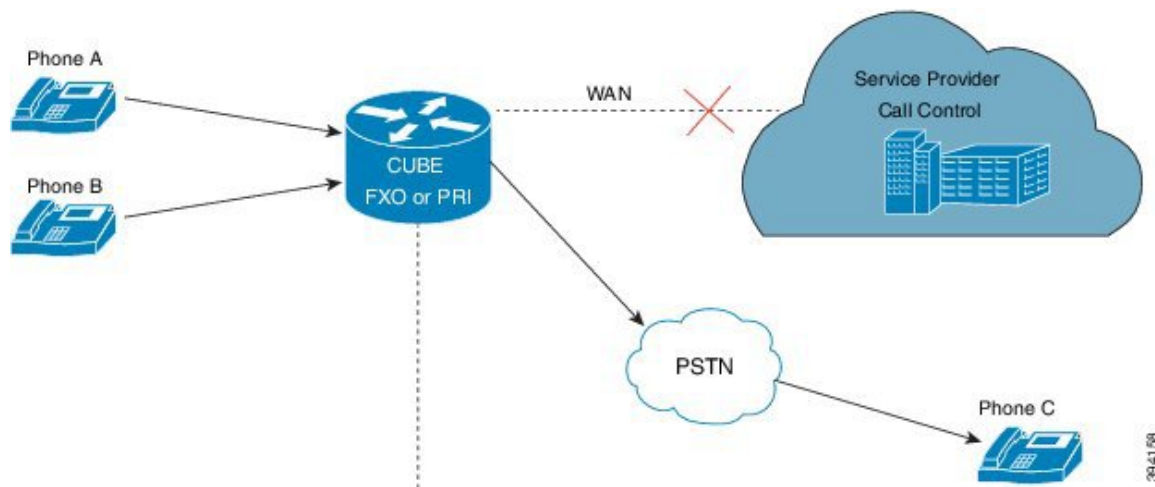
Survivability Support for Public Switched Telephone Network Access When WAN Is Down

If WAN link going down or registrar service unavailable, you can access the phones in the Public Switched Telephone Network (PSTN) through FXO or PRI cards that are configured on Cisco Unified Border Element (CUBE).



Note Survivability support for Public Switched Telephone Network (PSTN) access is supported only for CUBE running on Cisco 4000 Series Integrated Services Router.

Figure 79: Survivability Support for PSTN Access When WAN Is Down



394158

Example: Survivability Mode in P2P (regsync mode) when WAN is Down

```
CUBE# show sip-ua registration passthrough status
```

CallId	DirectoryNum	peer	mode	In-Exp	reg-I	Out-Exp	survival
38	NCPhone1008	1	p2p	3595 /3600	1	3600	regsync

Example: Survivability Mode in E2E (local fallback mode) when WAN is Down

```
CUBE# show sip-ua registration passthrough status
```

```
CallId    DirectoryNum    peer    mode    In-Exp    reg-I    Out-Exp    survival
=====    =====
70        NCPPhone1006    1       e2e     35 /70    --       0          locfall
=====
```

```
CallId    DirectoryNum    peer    mode    In-Exp    reg-I    Out-Exp    survival
=====    =====
513       NCPPhone1008    1       e2e     40 /70    --       0          locfall
=====
```

Feature Information for Survivability for Hosted and Cloud Services

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 104: Feature Information for Survivability for Hosted and Cloud Services

Feature Name	Releases	Feature Information
Survivability for Hosted and Cloud Services	Cisco IOS XE Fuji 16.9.1	Supports survivability for Hosted and Cloud Services .

Configure Survivability for Hosted and Cloud Services**Configure Local Fallback or Registration Synchronization Globally****SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. registration passthrough local-fallback tag
6. end

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice service VoIP configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# sip	Enters voice service SIP configuration mode.
Step 5	registration passthrough local-fallback tag Example: Device(conf-serv-sip)# registration passthrough local-fallback 10	Configures SIP registration passthrough for local fallback mode; this will locally respond to REGISTER in p2p mode when WAN is down. The <i>tag</i> is the WAN link or registrar server dial-peer tag. <ul style="list-style-type: none"> To configure the registration sync mode, you can use the registration passthrough reg-sync tag command. Use the static keyword to set the phone URL to p2p registration.
Step 6	end Example: Device(conf-serv-sip)# end	Returns to privileged EXEC mode.

Configure Local Fallback or Registration Synchronization at the Tenant Level

SUMMARY STEPS

1. enable
2. configure terminal
3. voice class tenant *tag*
4. registration passthrough local-fallback *tag*
5. exit
6. dial-peer voice *tag* voip
7. voice-class sip tenant *tag*
8. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	voice class tenant <i>tag</i> Example: <pre>Device(config)# voice class tenant 1</pre>	Enters voice class tenant configuration mode.
Step 4	registration passthrough local-fallback <i>tag</i> Example: <pre>Device(config-class)# registration passthrough local-fallback 10</pre>	Configures SIP registration passthrough for local fallback mode; this locally responds to REGISTER in p2p mode when WAN is down. The <i>tag</i> is the WAN link or registrar server dial-peer tag. <ul style="list-style-type: none"> • To configure the registration sync mode, you can use the registration passthrough reg-sync <i>tag</i> command. Use the static keyword to set the phone URL to p2p registration.
Step 5	exit Example: <pre>Device(config-class)# exit</pre>	Exits tenant configuration mode and returns to global configuration mode.
Step 6	dial-peer voice <i>tag</i> voip Example: <pre>Device(config)# dial-peer voice 444 voip</pre>	Enters dial peer voice configuration mode.
Step 7	voice-class sip tenant <i>tag</i> Example: <pre>Device(config-dial-peer)# voice-class sip tenant 1</pre>	Associates the dial-peer with the tenant.
Step 8	exit Example: <pre>Device(config-class)# exit</pre>	Exits dial-peer configuration mode and returns to global configuration mode.

Configure Local Fallback or Registration Synchronization on a Dial Peer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip registration passthrough local-fallback tag**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: <pre>Device(config)# dial-peer voice 4 voip</pre>	Enters dial peer VoIP configuration mode.
Step 4	voice-class sip registration passthrough local-fallback tag Example: <pre>Device(config-dial-peer)# voice-class sip registration passthrough local-fallback 10</pre>	Configures SIP registration passthrough for local fallback mode; this will locally respond to REGISTER in p2p mode when WAN is down. The <i>tag</i> is the WAN link or registrar server dial-peer tag. <ul style="list-style-type: none"> • To configure the registration sync mode, you can use the voice-class sip registration passthrough reg-sync tag command.
Step 5	end Example: <pre>Device(conf-serv-sip)# end</pre>	Returns to privileged EXEC mode.

Configuring Survivability for Phones Sending Single Register Request

The following configuration enables Cisco Unified Border Element (CUBE) to always check for the response from remote side. Request timeout on WAN side or response other than 200, 4XX, and 3XX received by CUBE from SBC enables the survivability.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **survivability single-register**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters voice service VoIP configuration mode.
Step 4	sip Example: <pre>Device(conf-voi-serv)# sip</pre>	Enters voice service SIP configuration mode.
Step 5	survivability single-register Example: <pre>Device(conf-serv-sip)# survivability single-register</pre>	Enables CUBE to always check for the response from the remote side. Request timeout on WAN side or response other than 200, 4XX, and 3XX received by CUBE from SBC enables the survivability.
Step 6	end Example: <pre>Device(conf-serv-sip)# end</pre>	Returns to privileged EXEC mode.

Configure OPTIONS Ping

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip options-keepalive up-interval value down-interval value**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: <pre>Device(config)# dial-peer voice 3 voip</pre>	Enters dial peer configuration mode.
Step 4	voice-class sip options-keepalive up-interval value down-interval value Example: <pre>Device(config-dial-peer)# voice-class sip options-keepalive up-interval 120 down-interval 120</pre>	Configures OPTIONS keepalive timer interval for DOWN and UP endpoints.
Step 5	end Example: <pre>Device(config-dial-peer)# end</pre>	Returns to privileged EXEC mode.

Configure Registration Timer

Perform the following task to configure the registration timer in the CUBE rather than on all SIP phones.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. registrar server expires max *value* min *value*
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters voice service VoIP configuration mode.
Step 4	sip Example: <pre>Device(conf-voi-serv)# sip</pre>	Enters voice service SIP configuration mode.
Step 5	registrar server expires max <i>value</i> min <i>value</i> Example: <pre>Device(conf-serv-sip)# registrar server expires max 300 min 200</pre>	Configures the maximum and minimum time (in seconds) for the registration expiry in CUBE. <ul style="list-style-type: none"> • If the phone sends expiry time as 600 seconds, then the CUBE will reply with 200 OK message and expiry time 300 seconds, and the phone will resend with expiry 300.
Step 6	end Example: <pre>Device(conf-serv-sip)# end</pre>	Returns to privileged EXEC mode.

Configuring the REGISTER Message Throttling in CUBE

Perform the following task to throttle the REGISTER message in CUBE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **registration passthrough rate-limit expires *value* local-fallback *tag***
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	voice service voip Example: <pre>Device(config)# voice service voip</pre>	Enters voice service VoIP configuration mode.
Step 4	sip Example: <pre>Device(conf-voi-serv)# sip</pre>	Enters voice service SIP configuration mode.
Step 5	registration passthrough rate-limit expires <i>value</i> local-fallback <i>tag</i> Example: <pre>Device(conf-serv-sip)# registration passthrough rate-limit expires 3600 local-fallback 3</pre>	Configures the SIP registration passthrough rate-limit expiry value for local-fallback (e2e). Although CUBE receives the REGISTER message every 5 minutes (300 seconds), it will send only one register message every one hour. <ul style="list-style-type: none"> • Under dial peer configuration mode, you can use the voice-class sip registration passthrough rate-limit expires <i>value</i> reg-sync <i>dial-peer-tag</i> command.
Step 6	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	<code>Device(conf-serv-sip)# end</code>	

Configure the Class of Restrictions (COR) List

Class of Restrictions (COR) provides the ability to deny certain call attempts based on the incoming and outgoing class of restrictions that are provisioned on the dial peers.

COR specifies which incoming dial peer can use which outgoing dial peer to make a call. You can provision each dial peer with an incoming and an outgoing COR list. The incoming COR list indicates the capability of the dial peer to initiate certain classes of calls. The outgoing COR list indicates the capability that is required for an incoming dial peer to deliver a call through this outgoing dial peer.

Before you begin

You must configure COR Groups. For more information, see [Dial Peer Configuration Guide](#).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *tag* voip**
4. **corlist incoming *dial-peer***
5. **corlist outgoing *dial-peer***
6. **description *string***
7. **destination-pattern *number***
8. **session protocol sipv2**
9. **session target registrar**
10. **voice-class sip registration passthrough local-fallback *tag***
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <code>Device> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <code>Device# configure terminal</code>	Enters global configuration mode.
Step 3	dial-peer voice <i>tag</i> voip Example:	Enters dial peer configuration mode.

	Command or Action	Purpose
	<code>Device(config)# dial-peer voice 3 voip</code>	
Step 4	corlist incoming <i>dial-peer</i> Example: <code>Device(config-dial-peer)# corlist incoming FromPhone</code>	Specifies the COR to be applied on an incoming dial peer (for incoming calls).
Step 5	corlist outgoing <i>dial-peer</i> Example: <code>Device(config-dial-peer)# corlist outgoing FromSP</code>	Specifies the COR to be applied for outgoing dial peer (for outgoing calls).
Step 6	description <i>string</i> Example: <code>Device(config-dial-peer)# description registration</code>	Adds a description to a dial peer.
Step 7	destination-pattern <i>number</i> Example: <code>Device(config-dial-peer)# destination-pattern 1111</code>	Specifies either the prefix or the full E.164 phone number to be used for the dial peer.
Step 8	session protocol sipv2 Example: <code>Device(config-dial-peer)# session protocol sipv2</code>	Specifies the session protocol for SIP calls between local and remote devices using the packet network.
Step 9	session target registrar Example: <code>Device(config-dial-peer)# session target registrar</code>	Specifies to route the call to the registrar endpoint for SIP dial peers.
Step 10	voice-class sip registration passthrough local-fallback <i>tag</i> Example: <code>Device(config-dial-peer)# voice-class sip registration passthrough local-fallback 5</code>	Configures SIP registration passthrough for local fallback mode.
Step 11	end Example: <code>Device(config-dial-peer)# end</code>	Returns to privileged EXEC mode.

Verify Survivability

The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show dial-peer voice summary**
3. **show sip-ua registration passthrough status**
4. **show sip-ua register status**
5. **show voip rtp connections**
6. **show call active voice compact**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show dial-peer voice summary

Displays the summary information for each voice dial peer.

Example:

```
Device# show dial-peer voice summary
```

```
dial-peer hunt 0
          AD
TAG      TYPE  MIN  OPER PREFIX  DEST-PATTERN  PRE PASS          OUT
1        voip  up   up      1111...      0  syst registrar
2        voip  up   down    1.....      0  syst ipv4:10.104.45.253  busyout
1000     voip  down down    9900...      0  syst ipv4:9.0.0.174:30601
101      voip  down down    1.....      0  syst ipv4:10.104.45.31
102      voip  down down    11.....      0  syst ipv4:10.104.45.253
300      voip  down down    .T           0  syst
400      voip  down down    11110...     0  syst registrar
```

Step 3 show sip-ua registration passthrough status

Displays information about the SIP user agent registration passthrough status. In the sample output shown below, the parameter In-Exp shows the remaining expiry time and the survival field parameters can be regsync, locfall, or normal.

Example:

```
Device# show sip-ua registration passthrough status
```

```
CallId      Line      peer      mode In-Exp      reg-I Out-Exp survival
=====
5300        1111008  1         e2e  1041 /1200  ----- 1200  normal *
5305        1111002  1         e2e  2847 /3000  ----- 3000  normal *
```

```
5311          1111020      1          e2e 1070 /1200  ----- 1200   normal *
```

Step 4 show sip-ua register status

Displays information about the SIP user agent register status.

Example:

```
Device# show sip-ua register status
```

```
Line          peer  expires(sec)  reg survival P-Associ-URI
=====
11123         23    59            yes  regsync
```

Step 5 show voip rtp connections

Displays Real-Time Transport Protocol (RTP) named event packets.

Example:

```
Device# show voip rtp connections
```

```
VoIP RTP Port Usage Information:
Max Ports Available: 8091, Ports Reserved: 101, Ports in Use: 2
Port range not configured, Min: 16384, Max: 32767
```

Ports	Ports	Ports
Media-Address	Range	Available
Reserved	In-use	
Default Address-Range		8091
101	2	

```
VoIP RTP active connections :
No. CallId    dstCallId  LocalRTP  RmtRTP  LocalIP          RemoteIP
1    5324      5325      16410   16464   9.40.1.168      9.40.1.173
2    5325      5324      16412   16528   9.40.1.168      9.40.1.174
Found 2 active RTP connections
```

Step 6 show call active voice compact

Displays the compact version of the call information for 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
          5324 ANS   T9      g711ulaw  VOIP      P1111008          9.40.1.173:16464
          5325 ORG   T9      g711ulaw  VOIP      P1111020          9.40.1.174:16528
```

Configuration Examples—Survivability for Hosted and Cloud Services

Example: Configuring Local Fallback Globally

In the following example, local fallback is configured at global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# registration passthrough local-fallback 10
Device(config-serv-sip)# end
```

Example: Configuring Local Fallback at the Tenant Level

In the following example, local fallback is configured for tenant 1 and is applied for dial-peer 444:

```
Device>enable
Device#configure terminal
Device(config)#voice class tenant 1
Device(config-class)#registration passthrough local-fallback 10
Device(config-class)#exit
Device(config)#dial-peer voice 444 voip
Device(config-dial-peer)#voice-class sip tenant 1
Device(config-class)# exit
```

Example: Configuring Local Fallback on a Dial Peer

In the following example, local fallback is configured on dial-peer 2.

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# voice-class sip registration passthrough local-fallback 10
Device(config-dial-peer)# end
```

Example: Configuring Survivability for Phones Sending Single Register Request

In the following example, survivability is configured for phones sending single register request:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
```

```
Device(conf-serv-sip)# survivability single-register
Device(config-serv-sip)# end
```

Example: Configuring OPTIONS Ping

In the following example, OPTIONS Ping is configured on dial-peer 3:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 3 voip
Device(config-dial-peer)# voice-class sip options-keepalive up-interval 120 down-interval
120
Device(config-dial-peer)# end
```

Example: Configuring the Registration Timer

In the following example, registration timer is configured with a expiration value of minimum 200 and maximum 300 seconds.

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# registrar server expires max 300 min 200
Device(conf-serv-sip)# end
```

Example: Configuring REGISTER Message Throttling

In the following example, REGISTER message throttling is configured:

```
Device>enable
Device#configure terminal
Device(config)#voice service voip
Device(conf-voi-serv)#sip
Device(conf-serv-sip)#registration passthrough rate-limit expires 3600 local-fallback 3
Device(conf-serv-sip)#end
```

Example: Configuring the COR List

In the following example, "FromPhone" and "FromSP" COR groups are configured and applied to dial-peer 2:

```
Device>enable
Device# configure terminal
Device(config)#dial-peer cor list FromPhone
Device(config-dp-corlist)#member 911
Device(config-dp-corlist)#member 1800
Device(config)#dial-peer cor list FromSP
```

```
Device(config-dp-corlist)#member 911
Device(config-dp-corlist)#member 1800
Device(config-dp-corlist)#exit
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# corlist incoming FromPhone
Device(config-dial-peer)# corlist outgoing FromSP
Device(config-dial-peer)# description registration
Device(config-dial-peer)# destination-pattern 1111
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target registrar
Device(config-dial-peer)# voice-class sip registration passthrough local-fallback 5
Device(config-dial-peer)# end
```




CHAPTER 75

SUBSCRIBE-NOTIFY Passthrough

- [Overview, on page 863](#)
- [Restrictions, on page 865](#)
- [Information About SUBSCRIBE-NOTIFY Passthrough, on page 865](#)
- [Configure SUBSCRIBE-NOTIFY Passthrough, on page 867](#)
- [Configuration Examples for SUBSCRIBE-NOTIFY Passthrough, on page 872](#)

Overview

The SUBSCRIBE-NOTIFY mechanism is used for implementation of features such as Message Waiting Indication (MWI), Shared Call Appearance, Multiple Caller Appearance, Busy Lamp Field, and so on.

In CUBE, the SUBSCRIBE-NOTIFY framework on Unified Communications (UC) products supports the following:

- Configurable and Selective Passthrough of SUBSCRIBE and NOTIFY transactions from phones with the normalization that is required for address or topology hiding and dialog content updates for “dialog” event subscription.
- Survivability mode handling of incoming SUBSCRIBE request for critical events.

The key attributes of the SUBSCRIBE-NOTIFY Passthrough feature are as follows:

- Message Passthrough Application (MPA)—The SIP MPA handles SUBSCRIBE-NOTIFY passthrough. This application maintains subscribe dialogs, and references the dial-peer database and registration passthrough configurations to route the initial SUBSCRIBE and unsolicited NOTIFY requests.
- Header Passthrough—All the non-mandatory headers in SUBSCRIBE-NOTIFY requests and responses are passed through from one endpoint to the other.
- Content Passthrough—The content bodies in SUBSCRIBE-NOTIFY requests are passed through transparently from one endpoint to the other.
- “Dialog” Event Content Manipulation—The content in the NOTIFY body for a dialog event is updated before passthrough when the dialog is maintained by the CUBE.
- Passthrough Configuration and Filtering—SUBSCRIBE-NOTIFY passthrough is configurable globally as well as under dial-peer, and can be configured for selected events using the configuration of an event list.

- **Error Passthrough for SUBSCRIBE-NOTIFY Requests**—When an error is received for a SUBSCRIBE-NOTIFY request, the error is passed through to the peer with the relevant headers.
- **Backward Compatibility**—The SIP MPA has the highest priority when SUBSCRIBE-NOTIFY passthrough is enabled. If passthrough is not enabled (either for all events or for a specific event), the current applications will control the incoming requests and responses.
- **401/407 Error Message Passthrough**—SIP message 401/407 is sent by the user-agent server (UAS) or end device to challenge messages like INVITE/REFER/SUBSCRIBE and request for endpoint credentials information. CUBE does not store endpoint credential information to act on behalf of phone or endpoint. To enable the passthrough of 401/407, you can enable the **error passthru** command at the global level. The messages 401/407 are in passthru mode for INVITE/REFER/SUBSCRIBE.

Feature Information

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 105: Feature Information for SUBSCRIBE-NOTIFY Passthrough

Feature Name	Releases	Feature Information
CUBE (SUBSCRIBE-NOTIFY Passthrough)	Cisco IOS XE Fuji 16.9.1	<p>The SUBSCRIBE-NOTIFY mechanism is used for implementation of features such as Message Waiting Indication (MWI), Shared Call Appearance, Multiple Caller Appearance, Busy Lamp Field, and so on.</p> <p>In CUBE, the SUBSCRIBE-NOTIFY framework on Unified Communications (UC) products supports the following:</p> <ul style="list-style-type: none"> • Configurable and Selective Passthrough of SUBSCRIBE and NOTIFY transactions from phones with the normalization required for address or topology hiding and dialog content updates for “dialog” event subscription. • Survivability mode handling of incoming SUBSCRIBE request for critical events.

Restrictions

- The SUBSCRIBE-NOTIFY passthrough framework can only pass through events when there is a one-to-one association between the incoming request and the outgoing location to which the request has been sent out. This means that either:
 - There should be an outbound dial-peer identified for the request received.
 - or
 - The outbound target for the request could be only a single registrar.
- The following use cases are not supported:
 - SUBSCRIBE-NOTIFY passthrough with hunting of outbound dial-peers to which the subscribe or notify requests need to be sent.
 - SUBSCRIBE-NOTIFY passthrough where an inbound dial-peer has peer-to-peer mode of registration passthrough enabled with more than one registrar (there will be no forking of Subscribe-Notify Requests)
 - Local subscribe handling of unsupported events when the remote registrar is unavailable. Local subscribe handling is only applicable to cases where the inbound dial-peer matching the subscribe has registration passthrough enabled with “local-fallback.”

Information About SUBSCRIBE-NOTIFY Passthrough

The key attributes of the SUBSCRIBE-NOTIFY Passthrough feature are as follows:

- **Message Passthrough Application (MPA)**—The SIP MPA handles SUBSCRIBE-NOTIFY passthrough. This application maintains subscribe dialogs, and references the dial-peer database and registration passthrough configurations to route the initial SUBSCRIBE and unsolicited NOTIFY requests.
- **Header Passthrough**—All the non-mandatory headers in SUBSCRIBE-NOTIFY requests and responses are passed through from one endpoint to the other.
- **Content Passthrough**—The content bodies in SUBSCRIBE-NOTIFY requests are passed through transparently from one endpoint to the other.
- **“Dialog” Event Content Manipulation**—The content in the NOTIFY body for a dialog event is updated before passthrough when the dialog is maintained by the CUBE.
- **Passthrough Configuration and Filtering**—SUBSCRIBE-NOTIFY passthrough is configurable globally as well as under dial-peer, and can be configured for selected events using the configuration of an event list.
- **Error Passthrough for SUBSCRIBE-NOTIFY Requests**—When an error is received for a SUBSCRIBE-NOTIFY request, the error is passed through to the peer with the relevant headers.
- **Backward Compatibility**—The SIP MPA has the highest priority when SUBSCRIBE-NOTIFY passthrough is enabled. If passthrough is not enabled (either for all events or for a specific event), the current applications will control the incoming requests and responses.

- 401/407 Error Message Passthrough—SIP message 401/407 is sent by the user-agent server (UAS) or end device to challenge messages like INVITE/REFER/SUBSCRIBE and request for endpoint credentials information. CUBE does not store endpoint credential information to act on behalf of phone or endpoint. To enable the passthrough of 401/407, you can enable the **error passthru** command at the global level. The messages 401/407 are in passthru mode for INVITE/REFER/SUBSCRIBE.

SUBSCRIBE-NOTIFY Passthrough Request Routing

The first step of request or response routing is for Cisco Unified Border Element (CUBE) to determine whether or not the request has to be passed through. When a new SUBSCRIBE or unsolicited NOTIFY request arrives, its headers are used to match an incoming dial-peer. If the incoming dial-peer has SUBSCRIBE-NOTIFY Passthrough (SNPT) enabled or if there is no incoming dial-peer and global SNPT is enabled for that event, then the request is handed off to be passed through. For solicited subscriptions, the passthrough check is applicable only to the initial SUBSCRIBE request; subsequent requests or responses are not checked and will be routed based on updated dialog parameters.

The second step is to determine the outbound destination of the SUBSCRIBE or unsolicited NOTIFY request.

- **First Pass: Outbound dial-peer match**—An outbound VoIP dial-peer is first matched based on the request headers (From, To, and Via), the Subscriber Number (userid in the To header), and the incoming dial-peer Class of Restrictions (CoR) if any. If there is a match, the request is routed to the session target.
- **Second Pass: Configured registrar for registration passthrough in peer-to-peer mode**—If no outbound dial-peer is found and the incoming dial-peer has registration passthrough enabled in static (peer-to-peer) mode with a single registrar configured, then the request is routed to the registrar address.
- **Third Pass: Configured registrar for registration passthrough in end-to-end mode**—If no outbound dial-peer is found and the incoming dial-peer has registration passthrough enabled in dynamic (end-to-end) mode:
 - If the request Uniform Resource Identifier (URI) has the CUBE IP address, the request is routed to the configured registrar if only a single registrar is configured.
 - If the request URI has a non-CUBE IP address, then the request is routed to that IP address.
- **Fourth Pass: Request URI-based routing**—If no outbound dial-peer is found and no registration passthrough is configured, the request URI is used to route the request if it does not point to the CUBE's IP address.

SUBSCRIBE-NOTIFY Passthrough Survivability Mode

In survivability mode, the CUBE could encounter the following scenarios:

- When the CUBE receives a line-seize (event) subscribe in survivability mode, it checks the line-seize queue to see if another phone has already seized the same line; if not, CUBE accepts the subscription, sends a NOTIFY response with State = Active, and starts the timer for expiration. In survivability mode, SUBSCRIBE received for any event other than line-seize is rejected.
- If another phone has already subscribed for the line, CUBE sends a 200 OK (request successful) response for the new subscribe, but a final NOTIFY to indicate that the subscription has been terminated.
- If the subscription timer expires without re-subscription from the phone, CUBE sends a final NOTIFY to remove the subscription.

- If a subscription is created in active mode, but re-subscriptions or unsubscriptions are received in survivability mode, then CUBE returns an error for this subscription.

Configure SUBSCRIBE-NOTIFY Passthrough

Configure an Event List

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-event** *number*
4. **event** *name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice class sip-event <i>number</i> Example: Device(config)# voice class sip-event 1	Enters voice class configuration mode and configures the list of events to be passed through.
Step 4	event <i>name</i> Example: Device(config-class)# event message-summary	Adds the name of the event to be added to the event list.
Step 5	end Example: Device(config-class)# end	Returns to privileged EXEC mode.

Configure SUBSCRIBE-NOTIFY Event Passthrough Globally

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. pass-thru subscribe-notify-events *tag*
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice class voip	Enters voice service VoIP configuration mode.
Step 4	sip Example: Device(conf-voi-serv)# sip	Enters voice service SIP configuration mode.
Step 5	pass-thru subscribe-notify-events <i>tag</i> Example: Device(conf-serv-sip)# pass-thru subscribe-notify-events 1	Configures SUBSCRIBE-NOTIFY passthrough event with the SIP event list tag number to be linked globally. <ul style="list-style-type: none"> • You can use the pass-thru subscribe-notify-events all command to configure passthrough for all SUBSCRIBE-NOTIFY events.
Step 6	end Example: Device(conf-serv-sip)# end	Returns to privileged EXEC mode.

Configure SUBSCRIBE-NOTIFY Event Passthrough at the Dial-Peer Level

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip pass-thru subscribe-notify-events tag`
5. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	dial-peer voice tag voip Example: <pre>Device(config)# dial-peer voice 123 voip</pre>	Enters dial peer voice configuration mode.
Step 4	voice-class sip pass-thru subscribe-notify-events tag Example: <pre>Device(config-dial-peer)# voice-class sip pass-thru subscribe-notify-events 1</pre>	Configures SUBSCRIBE-NOTIFY passthrough event with the SIP event list tag number to be linked globally. <ul style="list-style-type: none"> • You can use the voice-class sip pass-thru subscribe-notify-events all command to configure passthrough for all SUBSCRIBE-NOTIFY events.
Step 5	end Example: <pre>Device(conf-serv-sip)# end</pre>	Returns to privileged EXEC mode.

Verify SUBSCRIBE-NOTIFY Passthrough

Perform this task to verify the configuration for SUBSCRIBE-NOTIFY Passthrough and to verify the subscriptions created. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show dial-peer voice *number* | inc pass**
3. **show subscription asnl session active**
4. **show subscription sip**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show dial-peer voice *number* | inc pass

Displays the information for voice dial peers. The following sample output shows the configured SUBSCRIBE-NOTIFY passthrough event for a particular dial peer.

Example:

```
Device# show dial-peer voice 123 | inc pass

ip media DSCP = ef, ip media rsvp-pass DSCP = ef
ip video rsvp-none DSCP = af41, ip video rsvp-pass DSCP = af41
voice class sip pass-thru headers = system,
voice class sip pass-thru subscribe-notify-events = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip privacy-policy passthru = system,
voice class sip registration passthrough = System
voice class sip refer-to-passing = system
```

Step 3 show subscription asnl session active

Displays information about Application Subscribe/Notify Layer (ASNL)-based and non-ASNL-based SIP subscriptions.

Example:

```
Device# show subscription asnl session active

ASNL Active Subscription Records Details:
=====
Number of active subscriptions: 1
URL: sip:user@10.7.104.88
  Event Name : stress
  Session ID : 8
  Expiration Time : 50 seconds
  Subscription Duration : 5 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
```



```

Total Notifications Received : 2
Last response code : ASNL_NOTIFY_RCVD
Last error code : ASNL_NONE
First Subscription Time : 10:55:12 UTC Apr 9 2000
Last Subscription Time : 10:55:12 UTC Apr 9 2000
First Notify Time : 10:55:12 UTC Apr 9 2000
Last Notify Time : 10:55:17 UTC Apr 9 2000
Application that subscribed : stress
Application receiving notification: stress

```

Step 4 show subscription sip

Displays information about ASNL-based and non-ASNL-based SIP subscriptions.

Example:

```
Device# show subscription sip
```

```
ASNL Active Subscription Records Summary:
=====
```

```
Number of active subscriptions: 2
```

SubId	CallId	Proto	URL	Event
----	----	----	---	-----
1	N/A	ASNL_PROTO_SIP	"Plutus" <sip:1111003@primary>	all
2	N/A	ASNL_PROTO_SIP	sip:1111003@primaryappserver1	as-feature

Client	EXPIRES(sec)	EVENT
=====	=====	=====
1111003	0	as-feature-event
Client	EXPIRES(sec)	EVENT
=====	=====	=====
1234	0	message-summary

Tips to Troubleshoot

Use the following commands to troubleshoot SUBSCRIBE-NOTIFY Passthrough:

- debug mpa events
- debug mpa error
- debug ccsip messages
- debug asnl events
- debug asnl error
- debug ccsip all

Configuration Examples for SUBSCRIBE-NOTIFY Passthrough

Example: Configuring an Event List

The following example shows how to configure an event list and add an event to the list of events that have to be passed through.

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-event-list 1
Device(config-class)# event 1 message-summary
Device(config-class)# end
```

Example: Configuring SUBSCRIBE-NOTIFY Event Passthrough Globally

The following example shows how to configure the SUBSCRIBE-NOTIFY passthrough event and link the SIP event list tag number globally.

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# pass-thru subscribe-notify-events 1
Device(conf-serv-sip)# end
```

Example: Configuring SUBSCRIBE-NOTIFY Event Passthrough under a Dial Peer

The following example shows how to configure the SUBSCRIBE-NOTIFY passthrough event and link the SIP event list tag number under a dial peer.

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 123 voip
Device(config-dial-peer)# voice-class sip pass-thru subscribe-notify-events 1
Device(config-dial-peer)# end
```



PART **XIII**

Serviceability

- [VoIP Trace, on page 875](#)
- [Session Identifier, on page 883](#)
- [Call Quality Statistics, on page 893](#)
- [Monitor Voice Quality, on page 899](#)
- [CDR Accounting, on page 907](#)
- [SNMP Accounting, on page 909](#)



CHAPTER 76

VoIP Trace

- [Overview, on page 875](#)
- [Prerequisites, on page 877](#)
- [Restrictions, on page 877](#)
- [Benefits of VoIP Trace, on page 877](#)
- [Guide to use VoIP Trace Framework, on page 878](#)
- [Configuration Example for VoIP Trace, on page 879](#)
- [Syslog Messages, on page 882](#)

Overview

VoIP Trace is a Cisco Unified Border Element (CUBE) serviceability framework, which provides a binary trace facility for troubleshooting SIP call issues. The VoIP Trace framework records both successful and failed calls. All call trace data is stored in system memory. In addition to being stored in the system memory, data for calls with IEC errors is also written to the logging buffer.

The VoIP Trace feature is enabled by default and may be used to help troubleshoot issues, even in deployments with high call volumes.

You can configure VoIP Trace for CUBE using the **trace** configuration sub-mode under **voice service voip** configuration mode:

```
router (config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#?
Voip Trace submode commands:
default Set a command to its defaults
exit Exit from voice service voip trace mode
no Negate a command or set its defaults
shutdown Shut Voip Trace debugging
memory-limit Set limit based on memory used
```

Within the VoIP Trace sub-mode (**conf-serv-trace**), you can configure the following CLI commands:

- **memory-limit** [*platform* | *memory*]
- **no** [**shutdown**]

VoIP Trace is used for event logging and debugging of VoIP parameters. Using the VoIP Trace framework, the following information is recorded:

- SIP messages for SIP trunk to SIP trunk calls

- CCSIP messages, Events, and APIs for CUBE
- SIP Errors
- Call Control (Unified Communication flows processed by CUBE)
- FSM (Finite State Machine) states and events

VoIP Trace monitors and logs SIP signalling and call events in memory as they occur. In the event that a call error is detected, or calls fail with 3xx, 4xx or 5xx cause codes, these event details are written to the logging buffer after the call clears.



Note Traces for error calls are logged at the rate of up to five traces per second.

There's a configurable memory limit allocated for storage of traces in a VoIP Trace framework for CUBE. The maximum memory limit that you can configure for VoIP Trace is 1000 MB. By default, VoIP Trace will use up to 10% of the available platform memory. For example, if CUBE is used on a platform with 8GB of RAM, VoIP Trace will use up to 800MB for trace data. Once the trace memory limit is reached, older traces are overwritten and will no longer be available.

You can configure the trace memory limit using the CLI command **memory-limit** [*platform* | *memory*] under **trace** configuration sub-mode:

```
Router(conf-serv-trace)#memory-limit ?
<10-1000> Specify maximum memory limit in MB
platform Use 10 percent of available memory
```

To display the traces for a call, use the following show command:

- **show voip trace** {*call-id identifier* | *session-id identifier* | *sip-call-id identifier* | *correlator identifier* | *all* | *cover-buffers* | *statistics* | *detail* }

Feature Information

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 106: Feature Information

Feature Name	Releases	Feature Information
Tenant based Filtering for VoIP Trace	Cisco IOS XE Cupertino 17.8.1a	The show voip trace supports tenant based filtering for VoIP Trace.

Feature Name	Releases	Feature Information
VoIP Trace	Cisco IOS XE Amsterdam 17.3.2	VoIP Trace is a CUBE Serviceability framework for Event Logging and Debug Classification. The following commands are introduced: <ul style="list-style-type: none"> • trace • memory-limit [<i>platform</i> <i>memory</i>] • shutdown • show voip trace {<i>call-id identifier</i> <i>session-id identifier</i> <i>sip-call-id identifier</i> <i>correlator identifier</i> all cover-buffers statistics detail }
Cover Buffer Enhancements for VoIP Trace	Cisco IOS XE Dublin 17.12.1a	VoIP trace for SIP messages is enhanced to display cause code in the cover buffer.

Prerequisites

Cisco IOS XE Amsterdam 17.3.2, Cisco IOS XE Bengaluru 17.4.1a or a later release supported by CUBE.

Restrictions

- Unable to trace incoming calls if active calls exhaust the memory-limit.
- It is not possible to trace calls with a single SIP leg using the trace command.

Benefits of VoIP Trace

The following are some of the benefits of VoIP Trace Serviceability framework:

- Enabled by default
- Minimal CLI configuration requirement
- Minimal processing impact
- Automatic call error identification and trace logging based on IEC Errors
- Request-based manual call error identification and trace logging (filtered by call-ID, session-ID and so on)

Guide to use VoIP Trace Framework

The following are some of the usage guidelines for the VoIP trace Serviceability framework.

- Enable or disable your VoIP trace serviceability framework using the following CLI commands:
 - Enable—Configure **trace** under **voice service voip** configuration mode to enable your VoIP trace framework (**trace** is enabled by default).
 - Disable—Configure **shutdown** under **voip trace** configuration mode to disable your VoIP trace framework. To enable VoIP trace after it's disabled, configure the CLI command **no shutdown**.
- If you configure **shutdown** the VoIP trace serviceability framework:
 - Stops tracing for active calls.
 - Deletes all existing traces in the system memory.
- Monitors calls received after enabling VoIP trace.
- Traces stored in memory can be displayed using the show command **show voip trace** {*call-id identifier* | *session-id identifier* | *sip-call-id identifier* | *correlator identifier* | **all** | **cover-buffers** | **statistics** [**detail**]}
 - The show command displays traces for both active and disconnected calls.
 - The show command displays information only for the SIP leg.
 - For media forking, VoIP trace also displays information for forked legs.
 - Voice trace can be filtered by tenant tag.
- For the CLI command **memory-limit** [**platform** | *memory*]
 - Configure **memory-limit platform** to set 10% of the total memory available to the IOS processor at the time of configuring the command as VoIP trace memory limit.
 - Configure **memory-limit memory** to set a custom VoIP trace memory limit. Range is 10–1000 MB.
 - Configuration of custom memory-limit more than the available platform memory is not allowed. Configuration fails with an error message:

```
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#memory-limit 800
Error: Setting memory-limit more than available platform memory (732 MB) is not
allowed.
```

- Configuration of memory-limit more than the 10% of the available platform memory affects the system performance. Configuration is successful with a warning message:

```
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#memory-limit 100
Warning: Setting memory limit more than 10% of available platform memory (73
MB) will affect system performance.
```


- Reducing the memory-limit from an existing limit **resets** the VoIP trace data. Take copy of the **show voip trace statistics detail** and **show voip trace all** output data before reducing the memory-limit.
 - A confirmation message is displayed when you reduce the memory-limit from an existing limit:


```
Reducing the memory-limit clears all VoIP Trace statistics and data.
If you wish to copy this data first, enter 'no' to cancel,
otherwise enter 'yes' to proceed.
```
- Increasing the memory-limit does not impact the VoIP trace data.

**Note**

- VoIP trace is unable to trace incoming calls if active calls exhaust the memory-limit.
- To change the Timestamps displayed in the VoIP trace, configure the following:

```
router(config)#monitor event-trace timestamps datetime ?
localtime      Use local time zone for timestamps
msec           Include milliseconds in timestamp
show-timezone  Add time zone information to timestamp
```

Configuration Example for VoIP Trace

From Cisco IOS XE Cupertino 17.8.1a, VoIP Trace format has been updated:

- The colon (:) is used as a separator whenever **key: value** pair is displayed.
- The colon (:) is always followed by a space. For example, **Dir: Inbound, Peer-Tag: 10**.

The following is a sample voip trace log snippet from Cisco IOS XE Cupertino 17.8.1a:

```
----- Cover Buffer -----
Search-key      = 808808:8888:1
Timestamp       = *Aug 30 21:21:45.583
Buffer-Id       = 1
CallID          = 1
Peer-CallID     = 2
Correlator      = 1
Called-Number   = 8888
Calling-Number  = 808808
SIP CallID      = 1-24132@8.41.17.71
SIP Session ID  = aae2281a4212504a96131a56d26bf2ed
GUID            = 1CE915CE8002
-----
0: *Aug 30 21:21:45.583: //1/1CE915CE8002/CUBE_VT/SIP/Msg/ccsipDisplayMsg:
Received: SIP UDP message from 8.41.17.71:5099 to 8.44.25.45:5060
INVITE sip:8888@CUBE.com SIP/2.0
Via: SIP/2.0/UDP 8.41.17.71:5099;branch=z9hG4bK-24132-1-0
From: <sip:808808@8.41.17.71:5099>;tag=1
To: <sip:8888@8.44.25.45:5060>
Call-ID: 1-24132@8.41.17.71
CSeq: 1 INVITE
Contact: sip:808808@8.41.17.71:5099
```

```

Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp

v=0
o=user1 53655765 2353687637 IN IP4 8.41.17.71
s=my first call
i=Basic SDP Testing
u=http://www.cisco.com
e=Adithya M <aditm@cisco.com>
p=9880562910
c=IN IP4 8.41.17.71
t=0 0
m=audio 6001 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=sendrecv

2: *Aug 30 21:21:45.583: //1/1CE915CE8002/CUBE_VT/SIP/FSM/SPI-State-Change: Current State:
  STATE_NONE, Next State: STATE_IDLE, Current Sub-State: STATE_NONE, Next Sub-State: STATE_NONE
3: *Aug 30 21:21:45.588: //1/1CE915CE8002/CUBE_VT/SIP/MISC/Matched Dialpeer: Dir: Inbound,
  Peer-Tag: 251
4: *Aug 30 21:21:45.605: //1/1CE915CE8002/CUBE_VT/SIP/FSM/Offer-Answer: Event:
  E_SIP_INVITE_SDP_RCVD, Current State: S_SIP_EARLY_DIALOG_IDLE, Next State:
  S_SIP_EARLY_DIALOG_OFFER_RCVD
5: *Aug 30 21:21:45.606: //1/1CE915CE8002/CUBE_VT/SIP/FSM/IWF: Event: E_SIP_IWF_EV_RCVD_SDP,
  Current State: S_SIP_IWF_SDP_IDLE, Next State: S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT
6: *Aug 30 21:21:45.607: //1/1CE915CE8002/CUBE_VT/SIP/MISC/Media Stream Parameters: Stream
  Type: voice-only, Stream State: STREAM_ADDING, Negotiated Codec: g711alaw, Negotiated DTMF
  Type: inband-voice, Stream Index: 1

```



Note From Cisco IOS XE Dublin 17.12.1a, VoIP trace format is updated to include cause code in the cover buffer:

The following is a sample VoIP trace for request time out call leg:

```

----- Cover Buffer -----
Search-key      = 808808:6666:4
Timestamp      = Apr 27 09:54:54.491
CallID         = 4
Peer-CallID    = 5
Correlator     = NA
Called-Number  = 6666
Calling-Number = 808808
SIP CallID     = 1-18630@10.1.40.50
SIP SessionID  =
GUID           = 651A3C548005
Tenant         = 0
Cause-code     = recovery on timer expiry (102)
-----
//CUBE receives INVITE message from the client
Received:
INVITE sip:6666@CUBE.com SIP/2.0
Via: SIP/2.0/UDP 10.1.40.50:5082;branch=z9hG4bK-18630-1-0
From: sipp <sip:808808@10.1.40.50:5082>;tag=1
To: sut <sip:6666@10.2.10.10:5060>
Call-ID: 1-18630@10.1.40.50
CSeq: 1 INVITE
Contact: sip:808808@10.1.40.50:5082
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0

```

```

//CUBE reponds with 100 TRYING for the INVITE message received from the client
Sent:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.1.40.50:5082;branch=z9hG4bK-18630-1-0
From: sipp <sip:808808@10.1.40.50:5082>;tag=1
To: sut <sip:6666@10.2.10.10:5060>
Date: Thu, 27 Apr 2023 09:54:54 GMT
Call-ID: 1-18630@10.1.40.50
CSeq: 1 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-17.12.20230331.111639
Session-ID: 00000000000000000000000000000000;remote=e521d6e24ce1548b879c4bc674890b01
Content-Length: 0

//CUBE now forwards the INVITE message to the server
Sent:
INVITE sip:6666@10.1.40.50:5083 SIP/2.0
Via: SIP/2.0/UDP 10.2.10.10:5060;branch=z9hG4bK01D3E
From: "sipp " <sip:808808@10.2.10.10>;tag=48289-D57
To: <sip:6666@10.1.40.50>
Date: Thu, 27 Apr 2023 09:54:54 GMT
Call-ID: 6524756F-E41811ED-800B8CD8-819FA3D4@10.2.10.10
Supported: timer,resource-priority,replaces,sdp-anat,X-cisco-srtp-fallback
Min-SE: 1800
Cisco-Guid: 1696218196-3826782701-2147847384-2174723028
User-Agent: Cisco-SIPGateway/IOS-17.12.20230331.111639
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
CSeq: 101 INVITE
Timestamp: 1682589294
Contact: <sip:808808@10.2.10.10:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
P-Asserted-Identity: "sipp " <sip:808808@10.2.10.10>
Session-ID: e521d6e24ce1548b879c4bc674890b01;remote=00000000000000000000000000000000
Content-Length: 0

//If CUBE doesn't receive any response from the server after retransmission of INVITE
messages,
then CUBE replies back with '408 Request Timeout' to the client.

Sent:
SIP/2.0 408 Request Timeout
Via: SIP/2.0/UDP 10.1.40.50:5082;branch=z9hG4bK-18630-1-0
From: sipp <sip:808808@10.1.40.50:5082>;tag=1
To: sut <sip:6666@10.2.10.10:5060>;tag=57B32-43B
Date: Thu, 27 Apr 2023 09:54:54 GMT
Call-ID: 1-18630@10.1.40.50
CSeq: 1 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-17.12.20230331.111639
Reason: Q.850;cause=102
Session-ID: 00000000000000000000000000000000;remote=e521d6e24ce1548b879c4bc674890b01
Content-Length: 0

//The call is tear down with the ACK message received from the client
Received:
ACK sip:6666@10.2.10.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.1.40.50:5082;branch=z9hG4bK-18630-1-0
From: sipp <sip:808808@10.1.40.50:5082>;tag=1
To: sut <sip:6666@10.2.10.10:5060>;tag=57B32-43B
Call-ID: 1-18630@10.1.40.50
CSeq: 1 ACK

```

```
Contact: <sip:sipp@10.1.40.50:5082;transport=UDP>
Max-Forwards: 70
Subject: Performance Test
Content-Length: 0
```

Syslog Messages

A syslog message is generated in the following format, when CUBE is configured to register with a SIP trunk:

SIP Trunk Registration Success

```
*Aug 12 08:50:41.922: %SIP-3-REG_INTERNAL: Registration Success.
Tenant=300;Number=slido123;registrar=dns:slido.com;addr=8.0.0.121;port=6123;connid=4
```

SIP Trunk Registration Failure

```
*Aug 12 08:50:41.876: %SIP-3-REG_INTERNAL: Registration failed.
Tenant=200;Number=Engineering2541_LGU;registrar=dns:xyz.cisco.com;addr=8.0.0.121;port=9072;connid=3
```



Note

- The syslog message is logged whenever there is change in registration status (from success to failure and vice-versa).
 - If there are consecutive successful or failure responses, only the first successful or failure response is logged.
-



CHAPTER 77

Session Identifier

- [Overview, on page 883](#)
- [Configure Support for Session Identifier, on page 885](#)
- [Tips to Troubleshoot, on page 885](#)

Overview

Cisco Unified Border Element (CUBE) supports “Session Identifier” for end-to-end tracking of a SIP session in IP-based multimedia communication systems. Support for session identifier is in compliance with RFC 7206 and draft-ietf-insipid-session-id-15.

CUBE supports “Session Identifier” that overcomes the limitations with the existing call-identifiers and allows end-to-end tracking of a SIP session. To support session identifier, “Session-ID” header is added in the SIP request and response messages.



Note H.323 protocol is no longer supported from Cisco IOS XE Bengaluru 17.6.1a onwards. Consider using SIP for multimedia applications.



Note "Session Identifier" refers to the value of the identifier, whereas "Session-ID" refers to the header field used to convey the identifier.

The Session-ID comprises of Universally Unique Identifier (UUID) for each user agent participating in a call. Each call consists of two UUID known as local UUID and remote UUID. Local UUID is the UUID generated from the originating user agent and remote UUID is generated from the terminating user agent. The UUID values are presented as strings of lower-case hexadecimal characters, with the most significant octet of the UUID appearing first. Session Identifier comprises of 32 characters and remains same for the entire session. Refer to RFC 4122 for more information on UUID.

Example for Session ID header

```
Session-ID: ab30317f1a784dc48ff824d0d3715d86; remote=47755a9de7794ba387653f2099600ef2
```

In the above example:

Local UUID =

ab30317f1a784dc48ff824d0d3715d86

Remote UUID =

47755a9de7794ba387653f2099600ef2

Feature Behavior

- If all the user agents associated with CUBE support session-id, then CUBE allows pass-through of the Session ID header in all SIP request and response messages for the session.
- CUBE looks for the Session ID header present in the SIP messages and validates the SessionID header syntax as defined in draft-ietf-insipid-session-id-15. Session ID format earlier to draft-ietf-insipid-session-id-15 is considered as unsupported.
- If some of the user agents do not support session ID, CUBE generates local UUID on behalf of the user agent and sends the generated UUID in SIP request and response. CUBE generates UUID based on version 5 (SHA-1).
- If a Session ID is received in the format as defined in RFC 7329, CUBE considers it as unsupported. CUBE generates local UUID on behalf of the user agent and sends the generated UUID in SIP request and response.
- In a mid call scenario, where user a session is switched from supporting session identifier to non-supporting session identifier, CUBE saves the previous non-NULL session identifier and sends the saved non-NULL session identifier in re-invite messages as needed.
- For high availability, session ID is check pointed in active and re-created in standby.

Feature Information

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 107: Feature Information for Session Identifier Support

Feature Name	Releases	Feature Information
Support for Session Identifier	Baseline Functionality	<p>A new keyword session-id is added to the following commands:</p> <ul style="list-style-type: none"> • show call active voice • show call active video • show call history voice • show call history video • show call active voice brief • show call active video brief

Configure Support for Session Identifier

Session Identifier support is enabled on CUBE by default. No additional configuration required.

Tips to Troubleshoot

The following show commands helps you to troubleshoot any issues with session identifier.

- **show call active voice session-id WORD**
- **show call active voice brief session-id WORD**
- **show call active video session-id WORD**
- **show call active video brief session-id WORD**

WORD can be complete session identifier (local, remote, or both), or wildcard pattern of local or remote UUID. The valid wildcard patterns for search are *, 0-9, a-f, A-F.

The following session identifier is considered in the below examples:

```
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
```

Valid Search Patterns

You can search for the session identifier using complete Session ID header as shown below:

```
Device# show call active voice session-id db248b6cbdc547bbc6c6fdfb6916eeb;
remote=4fd24d9121935531a7f8d750ad16e19
```

```

Telephony call-legs: 0
SIP call-legs: 1
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

```

You can search for the session identifier using complete local UUID as shown below:

```

Device# show call active voice session-id db248b6cbdc547bbc6c6fdb6916eeb
Telephony call-legs: 0
SIP call-legs: 1
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

```

You can search for the session identifier using complete remote UUID as shown below:

```

Device# show call active voice session-id 4fd24d9121935531a7f8d750ad16e19
Telephony call-legs: 0
SIP call-legs: 1
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

```

You can search for session id using wildcard pattern match as shown below:

```

Device# Device# show call active voice session-id 4fd2*
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=4fd24d9121935531a7f8d750ad16e19
SessionIDRemoteuuid=db248b6cbdc547bbc6c6fdb6916eeb
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19

```



```
.
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

Device# show call active voice session-id *f*16*
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=4fd24d9121935531a7f8d750ad16e19
SessionIDRemoteuuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

Device# show call active voice brief session-id *
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=4fd24d9121935531a7f8d750ad16e19
SessionIDRemoteuuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

Device# show call active voice session-id *; remote=*
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=4fd24d9121935531a7f8d750ad16e19
SessionIDRemoteuuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

```

Device# show call active voice session-id 4fd24d9*;remote=*16eeb
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=4fd24d9121935531a7f8d750ad16e19
SessionIDRemoteuuid=db248b6cbdc547bbc6c6fd6fb6916eeb
.
.
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

```

Example: Invalid Search Patterns

The following wild card search patterns are invalid:

```

Device# show call active voice session-id ;remote=
Invalid Pattern. Pattern can have a string with ^[0-9a-fA-F*]+$ only OR a string with
^[0-9a-fA-F*];remote=[0-9a-fA-F*]+$ .

```

```

Device# show call active voice session-id *;remote=
Invalid Pattern. Pattern can have a string with ^[0-9a-fA-F*]+$ only OR a string with
^[0-9a-fA-F*];remote=[0-9a-fA-F*]+$ .

```

```

Device# show call active video session-id ;remote=*
Incorrect format for Session-ID Wildcard Pattern regular expression must be of the form
^[0-9A-Fa-f*]+$
Invalid Pattern. Pattern can have a string with ^[0-9a-fA-F*]+$ only OR a string with
^[0-9a-fA-F*];remote=[0-9a-fA-F*]+$ .

```

```

Device# show call active voice session-id 4fd24d9*remote=*16eeb
Incorrect format for Session-ID Wildcard Pattern regular expression must be of the form
^[0-9A-Fa-f*]+$
Invalid Pattern. Pattern can have a string with ^[0-9a-fA-F*]+$ only OR a string with
^[0-9a-fA-F*];remote=[0-9a-fA-F*]+$ .

```

Example: Search using Null session identifier

If one of the session identifier is null, you can search for the session identifiers using 0 as wildcard pattern. The following session identifier is considered in the below example:

```

SessionIDLocaluuid=00000000000000000000000000000000
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19

```

```

Device# show call active voice session-id 0
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
.
.
.
SessionIDLocaluuid=00000000000000000000000000000000
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
.
.
.

```

```
.
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Example: Correlation between Session Identifier and Call Identifier

The following session identifier is considered in the below examples:

```
SessionIDLocaluuid=db248b6cbdc547bbc6c6fdfb6916eeb
SessionIDRemoteuuid=4fd24d9121935531a7f8d750ad16e19
```

You can search for session identifier using the local UUID as shown below:

```
Device# show call active voice session-id d82c680a3eaecd5c29ac6ceaaa225061
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
.
.
.
.
VOIP:
ConnectionId[0x8CDAC180 0x10000 0x1B7 0x5B56400A]
IncomingConnectionId[0x8CDAC180 0x10000 0x1B7 0x5B56400A]
CallID=1022
GlobalCallId=[0xC3DAB665 0x770C11E5 0x80318550 0x5A000ED7]
SessionIDLocaluuid=d82c680a3eaecd5c29ac6ceaaa225061
SessionIDRemoteuuid=6497636d0b747785241cfbf5aa225064
CallReferenceId=0
CallServiceType=Unknown
RTP Loopback Call=FALSE
RemoteIPAddress=10.64.86.91
RemoteUDPPort=16614
RemoteSignallingIPAddress=10.64.86.91
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.127.17.142
RemoteMediaPort=16614
CoderTypeRate=g711ulaw
.
.
.
GlobalCallId=[0xC3DAB665 0x770C11E5 0x80318550 0x5A000ED7]
SessionIDLocaluuid=6497636d0b747785241cfbf5aa225064
SessionIDRemoteuuid=d82c680a3eaecd5c29ac6ceaaa225061
RemoteIPAddress=10.64.86.91
RemoteUDPPort=21978
RemoteSignallingIPAddress=10.64.86.91
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.127.17.188
RemoteMediaPort=21978
```

From the above output, you get to know that 1022 (highlighted) is the call identifier associated with the local session identifier **d82c680a3eaecd5c29ac6ceaaa225061**. You can now use this call identifier to get further details and debugging of the desired call as shown below:

```
Device# show sip-ua calls callid 1022
```

```

SIP CALL INFO of CCAPI callid 1022
Call 1
SIP Call ID           : 8cdac180-627159d8-9cd-5b56400a@10.64.86.91
State of the call     : STATE_ACTIVE (7)
Substate of the call  : SUBSTATE_NONE (0)
Calling Number        : 4443332212
Called Number         : 4443332211
Called URI            : sip:4443332211@10.64.86.132:5060
Bit Flags             : 0xC0401C 0x10000100 0x80004
CC Call ID           : 1022
Source IP Address (Sig) : 10.64.86.132
Destn SIP Req Addr:Port : [10.64.86.91]:5060
Destn SIP Resp Addr:Port : [10.64.86.91]:5060
Destination Name      : 10.64.86.91
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object       : 0x0
Media Mode            : flow-through
Media Stream 1
  State of the stream   : STREAM_ACTIVE
  Stream Call ID        : 1022
  Stream Type           : voice-only (0)
  Stream Media Addr Type : 1
  Negotiated Codec      : g711ulaw (160 bytes)
  Codec Payload Type    : 0
  Negotiated Dtmf-relay : inband-voice
  Dtmf-relay Payload Type : 0
  QoS ID                : -1
  Local QoS Strength    : BestEffort
  Negotiated QoS Strength : BestEffort
  Negotiated QoS Direction : None
  Local QoS Status      : None
  Media Source IP Addr:Port : [10.64.86.132]:16424
  Media Dest IP Addr:Port  : [10.127.17.142]:16614

Options-Ping      ENABLED:NO      ACTIVE:NO

SIP CALL INFO of peer leg CCAPI callid 1023
Call 2
SIP Call ID           : C3DEFC15-770C11E5-80348550-5A000ED7@10.64.86.132
State of the call     : STATE_ACTIVE (7)
Substate of the call  : SUBSTATE_NONE (0)
Calling Number        : 4443332212
Called Number         : 4443332211
Called URI            : sip:4443332211@10.64.86.91:5060
Bit Flags             : 0xC04018 0x90000100 0x80080
CC Call ID           : 1023
Source IP Address (Sig) : 10.64.86.132
Destn SIP Req Addr:Port : [10.64.86.91]:5060
Destn SIP Resp Addr:Port : [10.64.86.91]:5060
Destination Name      : 10.64.86.91
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object       : 0x0
Media Mode            : flow-through
Media Stream 1
  State of the stream   : STREAM_ACTIVE
  Stream Call ID        : 1023
  Stream Type           : voice-only (0)
  Stream Media Addr Type : 1
  Negotiated Codec      : g711ulaw (160 bytes)
  Codec Payload Type    : 0
  Negotiated Dtmf-relay : inband-voice

```

```

Dtmf-relay Payload Type : 0
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [10.64.86.132]:16426
Media Dest IP Addr:Port : [10.127.17.188]:21978

```

Example for video Calls

The following session identifier is considered in the below example:

```

SessionIDLocaluuid=6f0a93a3a79451aeb6d83f79a3359f
SessionIDRemoteuuid=a55b0f45861551b88f57d1fb5bb23f89

```



Note All the search patterns listed above for voice calls are also valid for video calls.

You can search for the session identifier using complete UUID (local, remote, or both) or use a wildcard pattern.

```
Device# show call active video session-id 6f*
```

```

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

GENERIC:
SetupTime=56399650 ms (*16:58:12.964 IST Thu Aug 20 2015)
Index=1
PeerAddress=sipp
PeerSubAddress=
PeerId=1
PeerIfIndex=14
LogicalIfIndex=0
ConnectTime=56400660 ms (*16:58:13.974 IST Thu Aug 20 2015)
CallDuration=00:00:56 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=video
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=0
VOIP:
ConnectionId[0x6083CB92 0x466511E5 0xFFFFFFFF8018F617 0xFFFFFFFFFA7C45A02]
IncomingConnectionId[0x6083CB92 0x466511E5 0xFFFFFFFF8018F617 0xFFFFFFFFFA7C45A02]
CallID=11
GlobalCallId=[0x6083F24F 0x466511E5 0xFFFFFFFF801BF617 0xFFFFFFFFFA7C45A02]
CallReferenceId=0
CallServiceType=Unknown
RTP Loopback Call=FALSE
SessionIDLocaluuid=6f0a93a3a79451aeb6d83f79a3359f
SessionIDRemoteuuid=a55b0f45861551b88f57d1fb5bb23f89
RemoteIPAddress=10.64.86.70
RemoteSignallingIPAddress=10.64.86.70

```

```
RemoteSignallingPort=5061  
RemoteMediaIPAddress=10.64.86.70  
RemoteMediaPort=6003  
RoundTripDelay=0 ms  
tx_DtmfRelay=inband-voice  
FastConnect=FALSE
```



CHAPTER 78

Call Quality Statistics

- [Overview, on page 893](#)
- [Restrictions, on page 895](#)
- [Configure Call Quality Parameters, on page 895](#)
- [Configuration Example for Call Quality Statistics, on page 897](#)

Overview

Call quality statistics in CUBE, such as packet loss, jitter, and round trip delay can be added to the call detail record (CDR), and these voice metrics can be calculated in IOS. For more information, refer to [Voice Quality Enhancements on Cisco Unified Border Element](#).

The call quality statistics feature is enhanced to provide the following capabilities:

- Enable or disable Quality of Service (QoS) for CUBE.
- Enable or disable Real-time Transport Protocol (RTP) Control Protocol (RTCP) passthrough.
- Configure call quality criteria parameters.

Call quality configuration parameters include `max_dropout`, `max_reorder`, and `clock_rate`. A maximum of three codecs (`codec_number`, `payload_type`, `clock_rate`) per media flow is collected by the PI and sent to CPP, which uses these values in statistics calculation. Calculated statistics such as Jitter, Packet Loss, and Delay are then fetched from the CPP to the CDR. These statistics can be viewed in the command line interface.

The CDR has the following data per call leg of the call:

- Packet Loss-Calculated based on methods shown in RFC3550. The RTCP sender/receiver reports are recalculated, and not just copied from the inbound leg to the outbound leg.
- Delay-Calculated based on timestamp received or timestamp of packets sent.
- Jitter-Variation of delay.

For more information on how to calculate the voice quality metrics related to media(voice) quality, such as conversational mean opinion score (MOS), jitter, and so on, see <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-call-monitoring.html>.

The VQM (Voice Quality Monitor) gives information on the voice quality metrics. The VQM on Cisco IOS XE platforms enables statistics gathering based on the received RTCP packets. From these statistics, a voice

quality measurement is developed to show the quality of the call. The output is in a simple format, using a system of good, poor, and bad types of ratings.

The following metrics exist in Call Detail Record (CDR) and Management Information Base (MIB) in CUBE, indicating voice quality:

1. MOSQe (conversational quality MOS)
2. Round-trip-delay.
3. Receive-delay (current jitter buffer size).
4. Packet-Loss-Rate.

The CDR is sent at the end of a call if AAA accounting is configured.

A CDR example is as follows:

```
<MOS-Con>4.4072</MOS-Con>
```

```
<round-trip-delay>1 ms</round-trip-delay>
```

```
<receive-delay>64 ms</receive-delay>
```

```
<voice-quality-total-packet-loss>0.0000 %</ voice-quality-total-packet-loss>
```

Feature Information

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 108: Feature Information for Call Quality Statistics Enhancement

Feature Name	Releases	Feature Information
Call Quality Statistics Enhancement	Cisco IOS XE 3.14S	<p>Call quality statistics in CUBE, such as packet loss, jitter, and round trip delay can be added to the call detail record (CDR), and these voice metrics can be calculated in IOS. For more information, refer to Voice Quality Enhancements on Cisco Unified Border Element.</p> <p>The call quality statistics feature is enhanced to provide the following capabilities:</p> <ul style="list-style-type: none"> • Enable or disable Quality of Service (QoS) for CUBE. • Enable or disable Real-time Transport Protocol (RTP) Control Protocol (RTCP) passthrough. • Configure call quality criteria parameters.

Restrictions

- Only SIP-to-SIP call quality statistics calculation is supported.
- The RTCP field is not recalculated, as it is end-to-end statistics.
- The round trip delay is only retrieved by RTCP, which means the round trip delay is not calculated if there is no related RTCP.
- Only three codec types are supported for one media flow to calculate the jitter; considering the data path performance, these three codecs would be the maximum number in one cache line.
- Only one RTP synchronization source (SSRC) is supported concurrently per media flow, which is indicated in the m-line of the session description protocol (SDP).
- Round trip delay calculation for transcoding calls is not supported.

Configure Call Quality Parameters

Configure Call Quality Criteria Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **call-quality**
5. **max-dropout** *number-of-packets*
6. **max-reorder** *number-of-packets*
7. **clock-rate** *payload-type-number frequency*
8. **clock-rate dynamic-default** *frequency*
9. **exit**
10. **rtcp all-pass-through**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	voice service voip Example: Device(config)# voice service voip	Enters global VoIP configuration mode.
Step 4	call-quality Example: Device(conf-voi-serv)# call-quality	Enters call quality configuration mode; this is the global call quality of service setup.
Step 5	max-dropout <i>number-of-packets</i> Example: Device(conf-serv-call-quality)# max-dropout 300	Configures the acceptable out of sequence future packets to drop. The range is from 2 to 2000 packets. The default value is 100.
Step 6	max-reorder <i>number-of-packets</i> Example: Device(conf-serv-call-quality)# max-reorder 500	Configures the acceptable out of sequence late packets. The range is from 2 to 2000 packets. The default value is 100.
Step 7	clock-rate <i>payload-type-number frequency</i> Example: Device(conf-serv-call-quality)# clock-rate 5 1500	Sets the payload type number and frequency. Clock rate is the RTP timestamp field's sampling frequency.
Step 8	clock-rate dynamic-default <i>frequency</i> Example: Device(conf-serv-call-quality)# clock-rate dynamic-default 10000	(Optional) Changes the default clock rate for all the dynamic payload types. The frequency range (in Hz) is from 1000 to 192000. <ul style="list-style-type: none">• You have several options to set the clock rate, such as for the different codecs.
Step 9	exit Example: Device(conf-serv-call-quality)# exit	Exits to global VoIP configuration mode.
Step 10	rtcp all-pass-through Example: Device(conf-voi-serv)# rtcp all-pass-through	(Optional) Passes through all RTCP in data path.
Step 11	end Example: Device(conf-voi-serv)# end	Returns to privileged EXEC mode.

Tips to Troubleshoot

Use the following **debug** and **show** commands to enable the logs, which helps in debugging:

- **debug ccsip verbose**
- **debug voip fpi all**

- **debug platform hardware qfp active feature sbc dbe datapath all**
- **debug platform hard qfp act feature sbc dbe client all**
- **debug ccsip message**
- **debug ccsip info**
- **show call active voice**
- **show platform hardware qfp active feature sbc data path call *call-id***

The following are some show command outputs that would be useful in troubleshooting:

- **Device# show call active voice | include LostPackets**

LostPackets=0

LostPackets=36 ----> *//Lost packets detail present in **show call active voice** output. View the complete command output based on the filters such as call-id to check the packet loss for a particular call leg.*

- **Device# show call active voice | include PlayDelayJitter**

PlayDelayJitter=0

PlayDelayJitter=38 -----> *//Jitter detail present in **show call active voice** output. View the complete command output based on the filters such as call-id to check the Jitter for a particular call leg.*

Configuration Example for Call Quality Statistics

```
voice service voip
no ip address trusted authenticate
callmonitor
rtcp all-pass-through
media statistics
media bulk-stats
allow-connections sip to sip
call-quality
max-dropout 2
max-reorder 2
sip
g729 annexb-all
no call service stop
```




CHAPTER 79

Monitor Voice Quality

- [Overview, on page 899](#)
- [Prerequisites, on page 901](#)
- [Restrictions, on page 901](#)
- [Configure Voice Quality Monitoring, on page 902](#)

Overview

Call quality statistics in CUBE, such as packet loss, jitter, and round trip delay can be added to the call detail record (CDR), and these voice metrics can be calculated in IOS. For more information, refer to [Voice Quality Enhancements on Cisco Unified Border Element](#).

The call quality statistics feature is enhanced to provide the following capabilities:

- Enable or disable Quality of Service (QoS) for CUBE.
- Enable or disable Real-time Transport Protocol (RTP) Control Protocol (RTCP) passthrough.
- Configure call quality criteria parameters.

Call quality configuration parameters include `max_dropout`, `max_reorder`, and `clock_rate`. A maximum of three codecs (`codec_number`, `payload_type`, `clock_rate`) per media flow is collected by the PI and sent to CPP, which uses these values in statistics calculation. Calculated statistics such as Jitter, Packet Loss, and Delay are then fetched from the CPP to the CDR. These statistics can be viewed in the command line interface.

The CDR has the following data per call leg of the call:

- Packet Loss-Calculated based on methods shown in RFC3550. The RTCP sender/receiver reports are recalculated, and not just copied from the inbound leg to the outbound leg.
- Delay-Calculated based on timestamp received or timestamp of packets sent.
- Jitter-Variation of delay.

For more information on how to calculate the voice quality metrics related to media(voice) quality, such as conversational mean opinion score (MOS), jitter, and so on, see <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-call-monitoring.html>.

The VQM (Voice Quality Monitor) gives information on the voice quality metrics. The VQM on Cisco IOS XE platforms enables statistics gathering based on the received RTCP packets. From these statistics, a voice

quality measurement is developed to show the quality of the call. The output is in a simple format, using a system of good, poor, and bad types of ratings.

The following metrics exist in Call Detail Record (CDR) and Management Information Base (MIB) in CUBE, indicating voice quality:

1. MOSQe (conversational quality MOS)
2. Round-trip-delay.
3. Receive-delay (current jitter buffer size).
4. Packet-Loss-Rate.

The CDR is sent at the end of a call if AAA accounting is configured.

A CDR example is as follows:

```
<MOS-Con>4.4072</MOS-Con>
```

```
<round-trip-delay>1 ms</round-trip-delay>
```

```
<receive-delay>64 ms</receive-delay>
```

```
<voice-quality-total-packet-loss>0.0000 %</ voice-quality-total-packet-loss>
```

VQM Metrics

The following are the metrics exported by VQM:

Table 109: Quality Metrics

IOS VQM, Voice/Audio Description Quality Metric	Description
MOS-Con	The conversational quality MOS. Conversational quality indicates the impact of the quality of the transmission on the dynamics of conversational exchanges between two parties; such metrics take into account delay, echo, and recency.
round-trip-delay	The instantaneous round-trip delay. This may be obtained from the RTCP SR reports.
receive-delay	The minimum delay that will be applied to the packets received when using an adaptive jitter buffer.
voice-quality-total-packet-loss	The total number of packets lost by the jitter buffer in the RTP stream.

Feature Information

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 110: Feature Information for Voice Quality Monitoring and Voice Quality Statistics

Feature Name	Releases	Feature Information
Voice Quality Statistics	Cisco IOS XE Everest 16.5.1b	Voice quality statistics provides information about the quality of the voice TDM-IP call. This feature is already implemented on ISR-G2, and the feature gap is filled in ISR 4000 series.
Voice Quality Monitoring	Cisco IOS XE Denali 16.3.1	The Voice Quality Monitoring (VQM) feature provides information on the voice quality metrics related to media (voice) quality, such as conversational mean opinion score (MOS), packet loss rate, and so on. VQM enables you to monitor the quality of calls traversing your VoIP network, and you can diagnose the cause of voice quality issues and troubleshoot them.

Prerequisites

The following commands must be executed to configure the voice quality metrics:

- callmonitor
- rtcp all-pass-through
- media statistics
- media bulk-stats
- call-quality
 - max-dropout 2
 - max-reorder 2

Restrictions

- Only SIP-to-SIP call quality statistics calculation is supported.
- The RTCP field is not recalculated, as it is end-to-end statistics.
- The round trip delay is only retrieved by RTCP, which means the round trip delay is not calculated if there is no related RTCP.
- Only three codec types are supported for one media flow to calculate the jitter; considering the data path performance, these three codecs would be the maximum number in one cache line.

- Only one RTP synchronization source (SSRC) is supported concurrently per media flow, which is indicated in the m-line of the session description protocol (SDP).
- Round trip delay calculation for transcoding calls is not supported.
- VQM MOS values are not calculated for DSP based calls.
- MOS value shows 0 if endpoint does not send RTCP packets.
- The voice quality statistics covers only the TDM-IP call. The implementation focuses on filling the following statistics based on query response from DSP for TDM-SIP and TDM-H323 call:
 - RoundTripDelay
 - GapFillWithSilence
 - GapFillWithPrediction
 - GapFillWithInterpolation
 - GapFillWithRedundancy
 - HiWaterPlayoutDelay
 - LoWaterPlayoutDelay
 - PlayDelayJitter

Configure Voice Quality Monitoring

Enable Media Statistics Globally

Perform this task to globally enable media statistics in voice-service configuration mode to estimate the values for packet loss, jitter, and round-trip time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media statistics**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters voice service VoIP configuration mode.
Step 4	media statistics Example: Device(conf-voi-serv)# media statistics	Enables media statistics to estimate the values of packet loss, jitter, and Round Trip Time (RTT) statistics. <ul style="list-style-type: none"> • The statistics are displayed using the show voice history and show call active voice commands. • If the media statistics command is disabled, the values will be zero.
Step 5	end Example: Device(conf-voi-serv)# end	Returns to privileged EXEC mode.

Example: Configuring Media Statistics Globally

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# media statistics
Device(conf-voi-serv)# end
```

Example: CDR Enabled MOS Output

At the end of a call, the MOSQe output is displayed in CDR only if the **debug radius accounting** is enabled.

The **show log | sec MOS-Con** command displays the MOS-Con value as shown below:

```
Device# show log | sec MOS-Con

*Jan 21 22:31:42.313: RADIUS:   Cisco AVpair      [1]  16  "MOS-Con=4.2312"
*Jan 21 22:31:42.313: RADIUS:   Cisco AVpair      [1]  16  "MOS-Con=4.2312"
```

Verify

Perform this task to verify the configuration for voice quality monitoring. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show call active voice | include LostPackets**
3. **show call active voice | include ReceiveDelay**
4. **show call active voice brief | sec RTT**
5. **show call active voice stats | sec MC**

DETAILED STEPS**Step 1** **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show call active voice | include LostPackets**

Displays statistics on the CUBE if the Voice Quality Metrics feature is configured.

Example:

```
Device# show call active voice | include LostPackets

LostPackets=0
LostPackets=0
```

Step 3 **show call active voice | include ReceiveDelay**

Displays statistics on the CUBE if the Voice Quality Metrics feature is configured.

Example:

```
Device# show call active voice | include ReceiveDelay

ReceiveDelay=0
ReceiveDelay=0
```

Step 4 **show call active voice brief | sec RTT**

Displays a truncated version of call information for voice calls in CUBE if the Voice Quality Metrics feature is configured.

Note This command is not applicable for TDM-IP voice calls.

Example:

```
Device# show call active voice brief | sec RTT

IP 173.39.65.81:7078      SRTP: off  rtt:12ms pl:0/0ms  lost:0/0/0  delay:0/0/0ms  g711ulaw
TextRelay: off  Transcoded: No  ICE: Off
IP 10.127.17.141:18920  SRTP: off  rtt:12ms pl:0/0ms  lost:0/0/0  delay:0/0/0ms  g711ulaw
TextRelay: off  Transcoded: No  ICE: Off
```

Step 5 **show call active voice stats | sec MC**

Displays R-Factor Statistics (G.107 MOS) on the CUBE if the Voice Quality Metrics feature is configured. A sample output is provided below for a voice call using G.711ulaw, VAD on, and at 5 percent packet loss rate.

Example:

```
Device# show call active voice stats | sec MC
```

```
DSP/RF: ML=, MC=, R1=, R2=, IF=, ID=, IE=, BL=, R0=, VR=
DSP/RF: ML=4.2346, MC=4.2346, R1=92, R2=92, IF=0, ID=0, IE=0, BL=0, R0=93, VR=2.0
DSP/RF: ML=4.2346, MC=4.2346, R1=92, R2=92, IF=0, ID=0, IE=0, BL=0, R0=93, VR=2.0
```

The following is an example output for the SNMP MIB:

```
cmqVoIPCallActiveRxPred107RMosConv.8520964.1 = 423 (MC)
```

For more information on the SNMP MIB "[cmqVoIPCallActiveRxPred107RMosConv](#)", see [SNMP Object Navigator](#).

In the sample output, the following can be noted:

- ML for codec G.711ulaw is 4.2346.
- MC for codec G.711ulaw is 4.2346.
- IE for codec G.711 is 0.
- R0 is 93.

The following table defines the abbreviations used in the sample output.

Table 111: Router Output Definitions for the show call active voice stats command

Type	Abbreviation	Definition
DSP/RF: R-Factor Statistics (G.107 MOS)	ML	R-factor MOS listening quality objective
	MC	R-factor MOS-CQE
	R1	R-factor for LQ profile1
	R2	R-factor for LQ
	IF	Effective codec impairment (IeEff)
	ID	Delay factors
	IE	Codec baseline score (Ie)
	BL	Codec baseline (Bpl)
	R0	Nominal value for R0 (default)
	VR	R-Factor version

Tips to Troubleshoot

Use the following debug commands to troubleshoot the Voice Quality Monitoring feature:

- `debug voip rtp packets`
- `debug performance monitor`
- `debug radius accounting`

- **debug aaa accounting**



CHAPTER 80

CDR Accounting

- [Overview, on page 907](#)

Overview

Accounting is the method for collecting information used for billing, auditing, and reporting, such as user identities, start and stop times, number of packets, and number of bytes. Accounting enables you to track the services users are accessing, as well as the amount of network resources they are consuming. For more information on Call Detail Records (CDRs), see [CDR Accounting for Cisco IOS Voice Gateways](#).



CHAPTER 81

SNMP Accounting

- [Overview, on page 909](#)

Overview

SRTP-SRTP pass-through feature allows pass-through of encrypted media from one call-leg to the other.

Cisco Unified Border Element (CUBE) supports SIP calls between endpoints using Transport Layer Security (TLS) for SIP signaling encryption and Secure Real-Time Protocol (SRTP) to provide RTP media encryption. However, these two encryption mechanisms may not be deployed simultaneously, depending on the required call flow invoked on the associated configuration.

The following are conditions of the SRTP Passthrough feature:

- SRTP Passthrough must be configured on both legs of the call. If the target adjacency does not support SRTP Passthrough, then the call is rejected by error message 415 (Unsupported Media Type).
- "m= .. RTP/SAVP .." and a="crypto:..." fields coming in on an Invite from one adjacency are passed on in an Invite to the target adjacency.
- "m= ...RTP/SAVP..." is a required field in the Invite to trigger SRTP Passthrough behavior in the CUBE.

Pass-Through of Unsupported Crypto Suites



Note Effective from Cisco IOS XE Everest Release 16.5.1b, CUBE supports AEAD_AES_128_GCM and AEAD_AES_256_GCM crypto-suites. For more information, see [SRTP-SRTP Interworking](#).

CUBE supports transparent passthrough of all (supported and unsupported) crypto suites.

CUBE has the ability to pass across crypto attributes (containing any unsupported crypto suites) as well as media packets (encrypted with unsupported crypto suites).

If SRTP pass-thru feature is enabled, media interworking will not be supported. Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Feature Information

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 112: Feature Information for SRTP-SRTP Pass-Through

Feature Name	Releases	Feature Information
Support for SRTP-SRTP Basic calls	Baseline functionality	This feature introduced support for basic SRTP-SRTP pass-through calls.