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 NONINFRINGEMENT 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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.
## CONTENTS

### CHAPTER 1

**Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup**  
1
Finding Feature Information  
1
Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup  
1
Toll Fraud Prevention  
4

### CHAPTER 2

**SIP-to-SIP Extended Feature Functionality for Session Border Controllers**  
7
Finding Feature Information  
8
Prerequisites for SIP-to-SIP Extended Feature Functionality for Session Border Controllers  
8
Modem Passthrough over VoIP  
8
Prerequisites for the Modem Passthrough over VoIP Feature  
8
Restrictions for the Modem Passthrough over VoIP Feature  
9
Information about Configuring Modem Passthrough over VoIP  
9
How to Configure Modem Passthrough over VoIP  
10
    Configuring Modem Passthrough over VoIP Globally  
11
    Configuring Modem Passthrough over VoIP for a Specific Dial Peer  
12
Troubleshooting Tips  
14
Verifying Modem Passthrough over VoIP  
14
Monitoring and Maintaining Modem Passthrough over VoIP  
15
Configuration Examples  
15
Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers  
17

### CHAPTER 3

**Bandwidth-Based Call Admission Control**  
19
Finding Feature Information  
20
Restrictions for Bandwidth-Based Call Admission Control  
20
Information About Bandwidth-Based Call Admission Control  
20
    Maximum Bandwidth Calculation  
20
    Bandwidth Tables  
21
How to Configure Bandwidth-Based Call Admission Control 23

Configuring Bandwidth-Based Call Admission Control at the Interface Level 23

Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level 24

Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping 26

Configuring Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level 26

Configuring Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level 27

Verifying Bandwidth-Based Call Admission Control 28

Troubleshooting Tips 30

Configuration Examples for Bandwidth-Based Call Admission Control 30

Example: Configuring Bandwidth-Based Call Admission Control at the Interface Level 30

Example: Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level 31

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level 31

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level 31

Feature Information for Bandwidth-Based Call Admission Control 32

CHAPTER 4

Interworking Between RSVP Capable and RSVP Incapable Networks 35

Finding Feature Information 35

Prerequisites for Interworking Between RSVP Capable and RSVP Incapable Networks 36

Restrictions for Interworking Between RSVP Capable and RSVP Incapable Networks 36

How to Configure Interworking Between RSVP Capable and RSVP Incapable Networks 36

Configuring RSVP on an Interface 36

Configuring Optional RSVP on the Dial Peer 37

Configuring Mandatory RSVP on the Dial Peer 39

Configuring Midcall RSVP Failure Policies 40

Configuring DSCP Values 42

Configuring an Application ID 43

Configuring Priority 44

Troubleshooting for Interworking Between RSVP Capable and RSVP Incapable Networks Feature 45

Verifying Interworking Between RSVP Capable and RSVP Incapable Networks 46
CHAPTER 5
Cisco Resource Reservation Protocol Agent 49
Finding Feature Information 49
Prerequisites for Cisco Resource Reservation Protocol Agent 49
Configuring Cisco Resource Reservation Protocol Agent 50
Feature Information for Cisco Resource Reservation Protocol Agent 50

CHAPTER 6
SIP INFO Method for DTMF Tone Generation 51
Finding Feature Information 51
Prerequisites for SIP INFO Method for DTMF Tone Generation 51
Restrictions for SIP INFO Methods for DTMF Tone Generation 52
Information About SIP INFO Method for DTMF Tone Generation 52
How to Review SIP INFO Messages 52
Configuring for SIP INFO Method for DTMF Tone Generation 53
Troubleshooting Tips 53
Feature Information for SIP INFO Method for DTMF Tone Generation 54

CHAPTER 7
DTMF Events through SIP Signaling 57
Finding Feature Information 57
Prerequisites for DTMF Events through SIP Signaling 58
Restrictions for DTMF Events through SIP Signaling 58
DTMF Dialing 58
NOTIFY Messages 58
Configuring DTMF Events through SIP Signaling 59
Verifying SIP DTMF Support 60
Troubleshooting Tips 65
Feature Information for DTMF Events through SIP Signaling 65

CHAPTER 8
Call Progress Analysis Over IP-to-IP Media Session 69
Feature Information for Call Progress Analysis Over IP-IP Media Session 69
Restrictions for Call Progress Analysis Over IP-to-IP Media Session 70
Information About Call Progress Analysis Over IP-IP Media Session 71
Call Progress Analysis 71
CPA Events 71
CHAPTER 9
Codec Preference Lists 77
   Feature Information for Negotiation of an Audio Codec from a List of Codecs 77
   Codecs configured using Preference Lists 78
   Prerequisites for Codec Preference Lists 79
   Restrictions for Codecs Preference Lists 79
   How to Configure Codec Preference Lists 80
      Configuring Audio Codecs Using a Codec Voice Class and Preference Lists 80
      Disabling Codec Filtering 81
   Troubleshooting Negotiation of an Audio Codec from a List of Codecs 83
   Verifying Negotiation of an Audio Codec from a List of Codecs 83

CHAPTER 10
AAC-LD MP4A-LATM Codec Support on Cisco UBE 87
   Finding Feature Information 87
   Restrictions for AAC-LD MP4A-LATM Codec Support on Cisco UBE 88
   AAC-LD MP4A-LATM Codec Support on Cisco UBE 88
   How to Configure the MP4A-LATM Codec 89
      Configuring the MP4A-LATM Codec on a Dial Peer 89
      Configuring the MP4A-LATM Codec under Voice Class Codec 91
      Verifying an Audio Call 92
   Configuration Examples for AAC-LD MP4A-LATM Codec Support on Cisco UBE 93
      Example: Configuring the MP4A-LATM Codec under a Dial Peer 93
      Example: Configuring the MP4A-LATM Codec under Voice Class Codec 93
   Feature Information for AAC-LD MP4A-LATM Codec Support on Cisco UBE 94

CHAPTER 11
Multicast Music-on-Hold Support on Cisco UBE 95
   Prerequisites for Multicast Music-on-Hold Support on Cisco UBE 95
   Restrictions for Multicast Music-on-Hold Support on Cisco UBE 95
   Information About Multicast Music-on-Hold Support on Cisco UBE 96
Multicast Music-on-Hold 96
  How to Enable Multicast Music-on-Hold on Cisco UBE 96
    Enabling MMOH on Cisco UBE 96
    Verifying the MMOH Support on Cisco UBE 98
  Troubleshooting Tips 100
Configuration Examples for Multicast Music-on-Hold Support on Cisco UBE 101
  Example: Enabling MMOH on Cisco UBE 101
Feature Information for Multicast Music-on-Hold Support on Cisco UBE 103

CHAPTER 12

Network-Based Recording 105
  Feature Information for Network-Based Recording 105
  Restrictions for Network-Based Recording 106
  Information About Network-Based Recording Using CUBE 107
    Deployment Scenarios for CUBE-based Recording 107
  Open Recording Architecture 108
    Network Layer 109
    Capture and Media Processing Layer 109
    Application Layer 109
  Media Forking Topologies 110
    Media Forking with Cisco UCM 110
    Media Forking without Cisco UCM 110
  SIP Recorder Interface 111
    Metadata 111
  How to Configure Network-Based Recording 112
    Configuring Network-Based Recording (with Media Profile Recorder) 112
    Configuring Network-Based Recording (without Media Profile Recorder) 115
  Verifying the Network-Based Recording Using CUBE 117
Additional References for Network-Based Recording 131

CHAPTER 13

Video Recording - Additional Configurations 133
  Feature Information for Video Recording - Additional Configurations 133
  Information About Additional Configurations for Video Recording 134
    Full Intra-Frame Request 134
  How to Configure Additional Configurations for Video Recording 135
    Enabling FIR for Video Calls (Using RTCP of SIP INFO) 135
## Chapter 14: TDoS Attack Mitigation

- Configuring H.264 Packetization Mode 136
- Monitoring Reference files or Intra Frames 137
- Verifying Additional Configurations for Video Recording 138

### TDoS Attack Mitigation 141

- Finding Feature Information 141
- Information About TDoS Attack Mitigation 141
- How to Configure TDoS Attack Mitigation 142
  - Configuring a Trusted IP Address List for Toll-Fraud Prevention 142
  - Configuring TDoS Attack Mitigation 143
- Verifying TDoS Attack Mitigation 145
- Configuration Examples for TDoS Attack Mitigation 146
  - Example: Trusted IP Address List Configuration 146
  - Example: TDoS Attack Mitigation Configuration 146
- Feature Information for TDoS Attack Mitigation 147

## Chapter 15: Cisco Unified Communications Gateway Services—Extended Media Forking 149

- Feature Information for Cisco Unified Communications Gateway Services—Extended Media Forking 149
- Restrictions for Unified Communications Gateway Services—Extended Media Forking 150
- Information About Cisco Unified Communications Gateway Services 151
  - Extended Media Forking (XMF) Provider and XMF Connection 151
  - XMF Call-Based Media Forking 152
  - XMF Connection-Based Media Forking 152
  - Media Forking for SRTP Calls 153
    - Crypto Tag 153
    - Example of SDP Data sent in an SRTP Call 154
  - Multiple XMF Applications and Recording Tone 154
  - Forking Preservation 156
- How to Configure UC Gateway Services 157
  - Configuring Cisco Unified Communication IOS Services on the Device 157
  - Configuring the XMF Provider 160
  - Verifying the UC Gateway Services 161
  - Troubleshooting Tips 163
- Configuration Examples for UC Gateway Services 163
### CHAPTER 16 Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls 165

- Feature Information for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls 165
- Restrictions for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls 166
- Symmetric and Asymmetric Calls 167
- High Availability Checkpointing Support for Asymmetric Payload 168
- How to Configure Dynamic Payload Type Passthrough for DTMF and Codec Packets for SIP-to-SIP Calls 168
  - Configuring Dynamic Payload Type Passthrough at the Global Level 168
  - Configuring Dynamic Payload Type Passthrough for a Dial Peer 169
- Verifying Dynamic Payload Interworking for DTMF and Codec Packets Support 171
- Troubleshooting Tips 171
- Configuration Examples for Asymmetric Payload Interworking 172
  - Example: Asymmetric Payload Interworking—Passthrough Configuration 172
  - Example: Asymmetric Payload Interworking—Interworking Configuration 173

### CHAPTER 17 iLBC Support for SIP and H.323 175

- Finding Feature Information 175
- Prerequisites for iLBC Support for SIP and H.323 175
- Restrictions for iLBC Support for SIP and H.323 176
- Information About iLBC Support for SIP and H.323 176
- How to Configure an iLBC Codec 176
  - Configuring an iLBC Codec on a Dial Peer 176
  - Configuring an iLBC Codec in the Voice Class 178
- Verifying iLBC Support for SIP and H.323 179
- Feature Information for iLBC Support for SIP and H.323 180

### CHAPTER 18 DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating 183

- Finding Feature Information 183
Acoustic Shock Protection 189

Finding Feature Information 189
Restrictions for ASP 189
Information About ASP 190
Acoustic Shock Protection 190
How to Configure ASP 191
Creating the Media Profile for ASP 191
Creating the Media Profile to Enable ASP 192
Configuring the Media Class at a Dial Peer Level for ASP 193
Configuring the Media Class Globally for ASP 194
Verifying ASP 195
Troubleshooting Tips 196

Configuration Examples for the Acoustic Shock Protection Feature 196
Feature Information for Acoustic Shock Protection 197

Noise Reduction 199

Finding Feature Information 199
Prerequisites for Noise Reduction 199
Restrictions for NR 200
Information About NR 200
Noise Reduction 200
How to Configure NR 201
Creating the Media Profile for NR 201
CHAPTER 21

SIP Ability to Send a SIP Registration Message on a Border Element 209
Finding Feature Information 209
Prerequisites for SIP Ability to Send a SIP Registration Message on a Border Element 209
Configuring SIP Ability to Send a SIP Registration Message on a Border Element 210
Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element 211

CHAPTER 22

SIP Profiles 213
Feature Information for SIP Profiles 213
Information About SIP Profiles 215
  Important Characteristics of SIP Profiles 216
Restrictions for SIP Profiles 217
How to Configure SIP Profiles 218
  Configuring a SIP Profile to Manipulate SIP Request or Response Headers 219
  Configuring SIP Profile Using Rule Tag 220
  Configuring a SIP Profile for Non-standard SIP Header 223
  Upgrading or Downgrading SIP Profile Configurations 225
  Configuring a SIP Profile as an Outbound Profile 226
  Configuring a SIP Profile as an Inbound Profile 227
Verifying SIP Profiles 228
Troubleshooting SIP Profiles 229
Examples: Adding, Modifying, Removing SIP Profiles 230
  Example: Adding a SIP, SDP, or Peer Header 230
  Example: Modifying a SIP, SDP, or Peer Header 231
  Example: Remove a SIP, SDP, or Peer Header 233
  Example: Inserting SIP Profile Rules 234
  Example: Upgrading and Downgrading SIP Profiles automatically 234
Example: Modifying Diversion Headers 235
Example: Sample SIP Profile Application on SIP Invite Message 235
Example: Sample SIP Profile for Non-Standard SIP Headers 236

CHAPTER 23

Session Refresh with Reinvites 237
Finding Feature Information 237
Prerequisites for Session Refresh with Reinvites 237
Information about Session Refresh with Reinvites 238
How to Configure Session Refresh with Reinvites 238
Configuring Session refresh with Reinvites 238
Feature Information for Session Refresh with Reinvites 240

CHAPTER 24

SIP Stack Portability 241
Finding Feature Information 241
Prerequisites for SIP Stack Portability 241
Information About SIP Stack Portability 242
SIP Call-Transfer Basics 242
  Basic Terminology of SIP Call Transfer 242
  Types of SIP Call Transfer Using the Refer Message Request 245
Feature Information for SIP Stack Portability 253

CHAPTER 25

VoIP for IPv6 255
Finding Feature Information 255
Prerequisites for VoIP for IPv6 256
Restrictions for Implementing VoIP for IPv6 256
Information About VoIP for IPv6 257
  SIP Features Supported on IPv6 257
  SIP Voice Gateways in VolPv6 258
  VolPv6 Support on Cisco UBE 259
How to Configure VoIP for IPv6 264
Configuring VoIP for IPv6 264
  Shutting Down or Enabling VoIPv6 Service on Cisco Gateways 264
  Shutting Down or Enabling VoIPv6 Submodes on Cisco Gateways 265
  Configuring the Protocol Mode of the SIP Stack 266
  Disabling ANAT Mode 267
Verifying SIP Gateway Status 268

RTP Pass-Through 270

- Configuring IPv6 Support for Cisco UBE 271
- Verifying RTP Pass-Through 272

Configuring the Source IPv6 Address of Signaling and Media Packets 272

Configuring the SIP Server 274

Configuring the Session Target 275

Configuring SIP Register Support 276

Configuring Outbound Proxy Server Globally on a SIP Gateway 278

Configuring UDP Checksum 279

Configuring IP Toll Fraud 280

Configuring the RTP Port Range for an Interface 281

Configuring Message Waiting Indicator Server Address 283

Configuring Voice Ports 284

Configuring Cisco UBE Mid-call Re-INVITE Consumption 285

- Configuring Passthrough of Mid-call Signalling 285
- Configuring Passthrough SIP Messages at Dial Peer Level 286

Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE 288

Configuration Examples for VoIP over IPv6 290

- Example: Configuring the SIP Trunk 290

Troubleshooting Tips for VoIP for IPv6 290

Verifying and Troubleshooting Tips 291

- Verifying Cisco UBE ANAT Call Flows 291
- Verifying and Troubleshooting Cisco UBE ANAT Flow-Through Call 292
- Verifying Cisco UBE ANAT Flow-Around Calls 297
- Verifying VMWI SIP 302
- Verifying SDP Passthrough Configuration 303

Feature Information for VoIP for IPv6 307

CHAPTER 26 Interworking of Secure RTP calls for SIP and H.323 313

Finding Feature Information 313

Prerequisites for Interworking of Secure RTP calls for SIP and H.323 314

Restrictions for Interworking of Secure RTP calls for SIP and H.323 314

Feature Information for Configuring Interworking of Secure RTP Calls for SIP and H.323 315
Example Configuring Domain-Based Routing Support on the Cisco UBE 408

CHAPTER 36  URI-Based Dialing Enhancements 409
Finding Feature Information 409
Information About URI-Based Dialing Enhancements 409
Call Flows for URI-Based Dialing Enhancements 410
How to Configure URI-Based Dialing Enhancements 413
Configuring Pass Through of SIP URI Headers 413
Configuring Pass Though of Request URI and To Header URI (Global Level) 414
Configuring Pass Though of Request URI and To Header URI (Dial Peer Level) 415
Configuring Pass Through of 302 Contact Header 416
Configuring Pass Through of 302 Contact Header (Global Level) 416
Configuring Pass Through of 302 Contact Header (Dial Peer Level) 418
Deriving of Session Target from URI 419
Configuration Examples for URI-Based Dialing Enhancements 421
Example: Configuring Pass Though of Request URI and To Header URI 421
Example: Configuring Pass Though of Request URI and To Header URI (Global Level) 421
Example: Configuring Pass Though of Request URI and To Header URI (Dial Peer Level) 422
Example: Configuring Pass Through of 302 Contact Header 422
Example: Configuring Pass Through of 302 Contact Header (Global Level) 422
Example: Configuring Pass Through of 302 Contact Header (Dial Peer Level) 422
Example: Deriving Session Target from URI 422
Additional References for URI-Based Dialing Enhancements 423
Feature Information for URI-Based Dialing Enhancements 423

CHAPTER 37  Additional References 425
Related References 425
Standards 426
MIBs 427
RFCs 427
Technical Assistance 429

CHAPTER 38  Glossary 431
Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

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

Note

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

• Finding Feature Information, page 1
• Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup, page 1
• Toll Fraud Prevention, page 4

Finding Feature Information

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

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.

Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

This chapter contains the following configuration topics:
Cisco UBE (Enterprise) Prerequisites and Restrictions

Dial Plan Management

- Dial Peer Configuration on Voice Gateway Routers —
- Translation Rules —
- ENUM support
- Configuring Tool Command Language (Tcl) —
- Cisco Service Advertisement Framework (SAF) —

Configuring Call Admissions Control

- VoIP Call Admissions Control —

Resource Reservation Protocol (RSVP)

- Interworking Between RSVP Capable and RSVP Incapable Networks
- Cisco Resource Reservation Protocol Agent

Dual-Tone Multifrequency (DTMF) Support and Interworking

- SIP—INFO Method for DTMF Tone Generation
- DTMF Events through SIP Signaling
- Configuring SIP DTMF Features —
- H.323 RFC2833 - SIP NOTIFY

Codec Negotiation

- 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

Transcoding

- iLBC Support for SIP and H.323
- Negotiation of an Audio Codec From a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco UBE
Payload Type Interoperability

- Interworking Between RSVP Capable and RSVP Incapable Networks
- Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

Transrating

- DSP Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating

Voice Quality Controls


Fax/modem Support

- Modem passthrough

H.323 Video

- Cisco Unified Border Element Videoconferencing

SIP Video

- SIP Video Calls with Flow Around Media
- RTP Media Loopback for SIP Calls
- Configuring RTP Media Loopback for SIP Calls

Telepresence

- SIP Video Support for Telepresence Calls

Security Features

- Toll Fraud Prevention
- Access lists (ACLs)
- SIP—Ability to Send a SIP Registration Message on a Border Element
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 Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), 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 Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
• Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or 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 this feature on 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 allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. 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 (DNS)--If you are using DNS 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 DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the "Cisco IOS Unified Communications Toll Fraud Prevention" paper.
The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft
- Lawful Intercept
- Media Inactivity
- Modem Passthrough over VoIP, on page 8
- TCP and UDP interworking
- Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
- Transport Layer Security (TLS)

- Finding Feature Information, page 8
- Prerequisites for SIP-to-SIP Extended Feature Functionality for Session Border Controllers, page 8
- Modem Passthrough over VoIP, page 8
- Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers, page 17
Finding Feature Information

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

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

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Modem Passthrough over VoIP

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

Prerequisites for the Modem Passthrough over VoIP Feature

• VoIP enabled network.

• Cisco IOS Release 12.1(3)T must run on the gateways for the Modem Passthrough over VoIP feature to work.

• Network suitability to pass modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Cisco IOS feature Service Assurance Agent.

Cisco Unified Border Element

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

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

Restrictions for the Modem Passthrough over VoIP Feature

Cisco Unified Border Element (Enterprise)

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

Note

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

Information about Configuring Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature performs the following functions:

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

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

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

Passthrough Switchover
When the gateway detects a data modem, both the originating gateway and the terminating gateway roll over to G.711. The roll over to G.711 disables the high-pass filter, disables echo cancellation, and disables VAD. At the end of the modem call, the voice ports revert to the prior configuration and the digital signal processor (DSP) goes back to the state before switchover. You can configure the codec by selecting the g711alaw or g711ulaw option of the codec command.
See also the How to Configure Modem Passthrough over VoIP, on page 10 section in this document.

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

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

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

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

*Figure 1: Modem Passthrough Connection*

![Modem Passthrough Connection Diagram](image)

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

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

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

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

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

### Configuring Modem Passthrough over VoIP Globally

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

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

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

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

#### SUMMARY STEPS

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

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### How to Configure Modem Passthrough over VoIP

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> voice service voip</td>
<td>Enters voice-service configuration mode. Configures voice service for all the connections for the gateways.</td>
</tr>
</tbody>
</table>

**Example:**

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

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

**Example:**

```
Router(config)# modem passthrough nse payload-type 97 codec g711alaw redundancy maximum-sessions 3
```

| **Step 4** exit | Exits voice-service configuration mode. |

**Example:**

```
Device(conf-voi-serv)# exit
```

| **Step 5** exit | Exits global configuration mode. |

**Example:**

```
Device(config)# exit
```

### Configuring Modem Passthrough over VoIP for a Specific Dial Peer

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

For modem passthrough to operate, you must define VoIP dial peers on both gateways to match the call, for example, by using a destination pattern or an incoming called number. The modem passthrough parameters associated with those dial peers then will apply to the call.
When modem passthrough is configured individually for a specific dial peer, that configuration for the specific dial peer takes precedence over the global configuration.

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

### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> dial-peer voice number voip</td>
<td>Enters dial-peer configuration mode. Configures a specific dial peer in dial-peer configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# dial-peer voice 5 voip</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** modem passthrough {system | nse [payload-type number] codec {g711ulaw | g711alaw} [redundancy]}}       | Configures the Modem Passthrough over VoIP feature for a specific dial peer. The default behavior for the Modem Passthrough for VoIP feature in dial-peer configuration mode is `modem passthrough system`. As required, the gateway defaults to `no modem passthrough`.

When the `system` keyword is enabled, the following parameters are not available: `nse`, `payload-type`, `codec`, and `redundancy`. Instead the values from the global configuration are used.

The payload type is an optional parameter for the `nse` keyword. Use the same `payload-type number` for both the originating gateway and the terminating gateway. The `payload-type number` can be set from 96 to 119. If you do not specify the `payload-type number`, the `number` defaults to 100. When the `payload-type` is 100, and you use the `show running-config` command, the `payload-type` parameter does not appear.

Use the same codec type for both the originating gateway and the terminating gateway. `g711ulaw` codec is required for T1, and `g711alaw` codec is required for E1.
### Command or Action | Purpose
--- | ---
 | The redundancy keyword is an optional parameter for sending redundant packets for modem traffic.

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits dial-peer configuration mode and returns to the global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Device(config-dial-peer)# exit
```

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Device(config)# exit
```

### Troubleshooting Tips

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

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

### Verifying Modem Passthrough over VoIP

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

**SUMMARY STEPS**

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

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

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

Monitoring and Maintaining Modem Passthrough over VoIP

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# <code>show call active voice brief</code></td>
<td>Displays information for the active call table or displays the voice call history table. The brief option displays a truncated version of either option.</td>
</tr>
<tr>
<td>Device# <code>show dial-peer voice 15 summary</code></td>
<td>Displays configuration information for dial peers. The <code>number</code> argument specifies a specific dial peer from 1 to 32767. The summary option displays a summary of all dial peers.</td>
</tr>
</tbody>
</table>

Configuration Examples

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

```sh
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
voice service voip
  modem passthrough nse codec g711ulaw redundancy maximum-session 5
  
resource-pool disable
  
!
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username lab
ip ftp password lab
no ip domain-lookup
!
isdn switch-type primary-5ess
cns event-service server
  
```
mta receive maximum-recipients 0

controller T1 0
  framing esf
  clock source line primary
  linecode b8zs
  pri-group timeslots 1-24

controller T1 1
  shutdown
  clock source line secondary 1

controller T1 2
  shutdown

controller T1 3
  shutdown

interface Ethernet0
  ip address 1.1.2.2 255.0.0.0
  no ip route-cache
  no ip mroute-cache

interface Serial0:23
  no ip address
  encapsulation ppp
  ip mroute-cache
  no logging event link-status
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no peer default ip address
  no fair-queue
  no cdp enable
  no ppp lcp fast-start

interface FastEthernet0
  ip address 26.0.0.1 255.0.0.0
  no ip route-cache
  no ip mroute-cache
  load-interval 30
  duplex full
  speed auto
  no cdp enable
  ip classless
  ip route 17.18.0.0 255.255.0.0 1.1.1.1
  no ip http server

voice-port 0:D

dial-peer voice 1 pots
  incoming called-number 55511..
  destination-pattern 020..
  direct-inward-dial
  port 0:D
  prefix 020

dial-peer voice 2 voip
  incoming called-number 020..
  destination-pattern 55511..
  modem passthrough nse codec g711ulaw redundancy
  session target ipv4:26.0.0.2

line con 0
  exec-timeout 0 0
Feature Information for SIP-to-SIP Extended Feature Functionality for Session Border Controllers

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

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

Table 1: Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP-to-SIP Extended Feature Functionality for Session Border Controllers | 12.4(6)T | The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs).

In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element

The following commands were introduced or modified: modem passthrough (dial-peer); modem passthough (voice-service); show call active voice voice; show call history voice voice; show dial-peer voice; voice service.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-to-SIP Extended Feature Functionality for Session Border Controllers</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: <code>modem passthrough (dial-peer); modem passthrough (voice-service); show call active voice voice; show call history voice voice; show dial-peer voice; voice service.</code></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.3S</td>
<td></td>
</tr>
</tbody>
</table>
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. The Bandwidth-Based Call Admission Control feature is supported on Session Initiation Protocol (SIP) trunks of the Time Division Multiplexing (TDM) SIP gateway and the Cisco Unified Border Element (Cisco UBE).

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.

- Finding Feature Information, page 20
- Restrictions for Bandwidth-Based Call Admission Control, page 20
- Information About Bandwidth-Based Call Admission Control, page 20
- How to Configure Bandwidth-Based Call Admission Control, page 23
- Configuration Examples for Bandwidth-Based Call Admission Control, page 30
- Feature Information for Bandwidth-Based Call Admission Control, page 32
Finding Feature Information

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

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

Restrictions for Bandwidth-Based Call Admission Control

- Cisco UBE, 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 Telephone 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.

Information About Bandwidth-Based Call Admission Control

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

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 2: Audio Bandwidth Table

<table>
<thead>
<tr>
<th>Codec and Bit Rate (Kbps)</th>
<th>Codec Sample Size in Bytes</th>
<th>Voice Payload Size in Bytes</th>
<th>Voice Payload Size in Milliseconds</th>
<th>Packets Per Second</th>
<th>Bandwidth for IPv4 (excluding Layer 2) in Kbps</th>
<th>Bandwidth for IPv6 (excluding Layer 2) in Kbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 (64 Kbps)</td>
<td>80</td>
<td>160</td>
<td>20</td>
<td>50</td>
<td>80</td>
<td>88</td>
</tr>
<tr>
<td>G.729 (8 Kbps)</td>
<td>10</td>
<td>20</td>
<td>20</td>
<td>50</td>
<td>24</td>
<td>32</td>
</tr>
<tr>
<td>G.723.1 (6.3 Kbps)</td>
<td>24</td>
<td>24</td>
<td>30</td>
<td>33.3</td>
<td>17</td>
<td>22</td>
</tr>
<tr>
<td>G.723.1 (5.3 Kbps)</td>
<td>20</td>
<td>20</td>
<td>30</td>
<td>33.3</td>
<td>16</td>
<td>21</td>
</tr>
<tr>
<td>G.726 (32 Kbps)</td>
<td>20</td>
<td>80</td>
<td>20</td>
<td>50</td>
<td>48</td>
<td>56</td>
</tr>
<tr>
<td>G.726 (24 Kbps)</td>
<td>15</td>
<td>60</td>
<td>20</td>
<td>50</td>
<td>40</td>
<td>48</td>
</tr>
<tr>
<td>G.726 (16 Kbps)</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>50</td>
<td>32</td>
<td>40</td>
</tr>
<tr>
<td>G.728 (16 Kbps)</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>50</td>
<td>32</td>
<td>40</td>
</tr>
<tr>
<td>G722_64k (64 Kbps)</td>
<td>80</td>
<td>160</td>
<td>20</td>
<td>50</td>
<td>80</td>
<td>88</td>
</tr>
<tr>
<td>ilbc_mode_20 (15.2 Kbps)</td>
<td>38</td>
<td>38</td>
<td>20</td>
<td>50</td>
<td>31</td>
<td>39</td>
</tr>
</tbody>
</table>
### Table 3: Fax Bandwidth Table

<table>
<thead>
<tr>
<th>T.38 Fax Bit Rate</th>
<th>Redundancy</th>
<th>Maximum Bandwidth in Kbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>2400</td>
<td>None</td>
<td>8</td>
</tr>
<tr>
<td>2400</td>
<td>Redundancy</td>
<td>17</td>
</tr>
<tr>
<td>9600 (default)</td>
<td>None</td>
<td>16</td>
</tr>
<tr>
<td>9600 (default)</td>
<td>Redundancy</td>
<td>46</td>
</tr>
<tr>
<td>14400</td>
<td>None</td>
<td>20</td>
</tr>
<tr>
<td>14400</td>
<td>Redundancy</td>
<td>65</td>
</tr>
<tr>
<td>33600</td>
<td>None</td>
<td>40</td>
</tr>
<tr>
<td>33600</td>
<td>Redundancy</td>
<td>142</td>
</tr>
</tbody>
</table>
How to Configure Bandwidth-Based Call Admission Control

Configuring Bandwidth-Based Call Admission Control at the Interface Level

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

You can configure the Bandwidth-Based Call Admission Control feature for the following interfaces:

- ATM
- Ethernet (Fast Ethernet, Gigabit Ethernet)
- Loopback
- Serial

Note
Cisco recommends that you configure a bind media to associate a specific interface for SIP calls. Otherwise, the interface used for the calls will be 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Configuring 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 required for the calls exceeds the aggregate bandwidth threshold.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><em>Example:</em> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>call threshold interface type number int-bandwidth [class-map name [l2-overhead percentage]] [low low-threshold high high-threshold] [midcall-exceed]</strong></td>
</tr>
<tr>
<td><em>Example:</em> 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</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><em>Example:</em> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# dial-peer voice 44 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> session protocol sipv2</td>
<td>Configures the Bandwidth-Based Call Admission Control feature for SIP dial peers only.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# session protocol sipv2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> max-bandwidth bandwidth-value [midcall-exceed]</td>
<td>Configures the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth required for the calls exceed the aggregate bandwidth threshold.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# max-bandwidth 24 midcall-exceed</td>
<td>• 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.</td>
</tr>
</tbody>
</table>
Configuring 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 between 400 to 600. The default SIP error response code is 488.

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

### Configuring 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action

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

### Configuring 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>dial-peer voice tag {pots</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# dial-peer voice 88 voip</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>voice-class sip error-code-override cac-bandwidth failure {sip-status-code-number</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 500</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# end</td>
</tr>
</tbody>
</table>

### Verifying Bandwidth-Based Call Admission Control

Perform this task to verify the configuration for the Bandwidth-Based Call Admission Control feature on Cisco UBE. 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

<table>
<thead>
<tr>
<th>IF Type</th>
<th>Value</th>
<th>Low</th>
<th>High</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0 int-bandwidth</td>
<td>0</td>
<td>100</td>
<td>400</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

Step 3  show call threshold status

Example:

Device# show call threshold status

<table>
<thead>
<tr>
<th>Status</th>
<th>IF Type</th>
<th>Value</th>
<th>Low</th>
<th>High</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avail</td>
<td>GigabitEthernet0/0 int-bandwidth</td>
<td>0</td>
<td>100</td>
<td>400</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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
Accepteds Calls = 3, Refused Calls = 0,
Bandwidth CAC Accepted Calls = 3, Bandwidth CAC Refused Calls = 0

Displays information for the voice dial peer.

Troubleshooting Tips

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

- debug ccsip all
- debug voice capi 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 Cisco UBE 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 Cisco UBE 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
```
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 Cisco UBE 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 Cisco UBE for bandwidth-based CAC SIP error response code mapping at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-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 Cisco UBE 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
```
Feature Information for Bandwidth-Based Call Admission Control

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Bandwidth-Based Call Admission Control            | 15.2(2)T | The Bandwidth-Based Call Admission Control 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 prevent QoS degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized.  
The following commands were introduced or modified: call threshold interface, error-code-override, max-bandwidth, show call threshold, voice-class sip |
The Bandwidth-Based Call Admission Control 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 prevent QoS degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized.

The following commands were introduced or modified:

- `call threshold interface`
- `error-code-override`
- `max-bandwidth`
- `show call threshold`
- `voice-class sip`
Interworking Between RSVP Capable and RSVP Incapable Networks

The Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based Resource Reservation Protocol (RSVP) support for basic audio call and supplementary services on Cisco Unified Border Element (UBE). This feature improves the interoperability between RSVP and non-RSVP networks. RSVP functionality added to Cisco UBE helps you to reserve the required bandwidth before making a call.

This feature extends RSVP support to delayed-offer to delayed-offer and delayed-offer to early-offer calls, along with the early-offer to early-offer calls.

- Finding Feature Information, page 35
- Prerequisites for Interworking Between RSVP Capable and RSVP Incapable Networks, page 36
- Restrictions for Interworking Between RSVP Capable and RSVP Incapable Networks, page 36
- How to Configure Interworking Between RSVP Capable and RSVP Incapable Networks, page 36
- Troubleshooting for Interworking Between RSVP Capable and RSVP Incapable Networks Feature, page 45
- Verifying Interworking Between RSVP Capable and RSVP Incapable Networks, page 46
- Feature Information for Interworking Between RSVP Capable and RSVP Incapable Networks, page 47

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for Interworking Between RSVP Capable and RSVP Incapable Networks

- RSVP policies allow you to configure separate bandwidth pools with varying limits so that any one application, such as video, can consume all the RSVP bandwidth on a specified interface at the expense of other applications, such as voice, which would be dropped.
- To limit bandwidth per application, you must configure a bandwidth limit before configuring Support for the Interworking Between RSVP Capable and RSVP Incapable Networks feature. See the Configuring RSVP on an Interface, on page 36.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for Interworking Between RSVP Capable and RSVP Incapable Networks

The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature has the following restrictions:

- Segmented RSVP is not supported.
- Interoperability between Cisco UBE and Cisco Unified Communications Manager is not available.
- RSVP-enabled video calls are not supported.

How to Configure Interworking Between RSVP Capable and RSVP Incapable Networks

Configuring RSVP on an Interface

You must allocate some bandwidth for the interface before enabling RSVP. Perform this task to configure RSVP on an interface.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot / port
4. ip rsvp bandwidth [reservable-bw [max-reservable-bw] [sub-pool reservable-bw]]
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>interface type slot / port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# interface FastEthernet 0/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables RSVP for IP on an interface.</td>
</tr>
<tr>
<td>ip rsvp bandwidth [reservable-bw [max-reservable-bw] [sub-pool reservable-bw]]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ip rsvp bandwidth 10000 100000</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# end</td>
</tr>
</tbody>
</table>

**Configuring Optional RSVP on the Dial Peer**

Perform this task to configure optional RSVP at the dial peer level. This configuration allows you to have uninterrupted call even if there is a failure in bandwidth reservation.
### SUMMARY STEPS

1. enable  
2. configure terminal  
3. dial-peer voice `tag voip`  
4. no acc-qos `{controlled-load | guaranteed-delay} [audio | video]`  
5. req-qos `{controlled-load | guaranteed-delay} [audio | video] [bandwidth [default `bandwidth-value`] [max `bandwidth-value`]]`  
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
  Example:  
  Device> enable  
| 2    | configure terminal | Enters global configuration mode.  
  Example:  
  Device# configure terminal  
| 3    | dial-peer voice `tag voip` | Enters dial peer voice configuration mode.  
  Example:  
  Device(config)# dial-peer 77 voip  
| 4    | no acc-qos `{controlled-load | guaranteed-delay} [audio | video]` | Removes any value configured for the acc-qos command.  
  Example:  
  Device(config-dial-peer)# no acc-qos controlled-load  
  Keywords are as follows:  
  • controlled-load--Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.  
  • guaranteed-delay--Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.  
| 5    | req-qos `{controlled-load | guaranteed-delay} [audio | video] [bandwidth [default `bandwidth-value`] [max `bandwidth-value`]]` | Configures the desired quality of service (QoS) to be used.  
  Example:  
  Device(config-dial-peer)# req-qos controlled-load  
  • Calls continue even if there is a failure in bandwidth reservation.
Configuring Mandatory RSVP on the Dial Peer

Perform this task to configure Mandatory RSVP on the dial peer. This configuration ensures that the call does not connect if sufficient bandwidth is not allocated.

SUMMARY STEPS

1. enable
2. configure terminal
dial-peer voice tag voip
4. acc-qos {best-effort | controlled-load | guaranteed-delay} [audio | video]
5. req-qos {best-effort [audio | video] | {controlled-load | guaranteed-delay} [audio | video] [bandwidth [default bandwidth-value] [max bandwidth-value]]}
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Note: Configure the req-qos command using the same keyword that you used to configure the acc-qos command, either controlled-load or guaranteed-delay. That is, if you configured acc-qos controlled-load command in the previous step, then use the req-qos controlled-load command here.

Example:
Device(config-dial-peer)# req-qos controlled-load

(Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode.

Example:
Device(config-dial-peer)# end
### Configuring Midcall RSVP Failure Policies

Perform this task to enable call handling policies for a midcall RSVP failure.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>dial-peer voice tag voip</code></td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Device(config)# dial-peer 77 voip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>`acc-qos {best-effort</td>
<td>controlled-load</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Device(config-dial-peer)# acc-qos best-effort</code></td>
<td></td>
</tr>
</tbody>
</table>

- **Keywords** as follows:
  - `best-effort`--Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default.
  - `controlled-load`--Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.
  - `guaranteed-delay`--Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

| **Step 5**              | **Purpose**                                                            |
| `req-qos {best-effort [audio | video] | {controlled-load | guaranteed-delay} [audio | video] [bandwidth [default bandwidth-value] [max bandwidth-value]]` | Configures mandatory RSVP on the dial-peer.                     |
| **Example:**            | **Example:**                                                           |
| `Device(config-dial-peer)# req-qos controlled-load` |                                                                 |

- Calls continue even if there is a drop in the bandwidth reservation.

| **Step 6**              | **Purpose**                                                            |
| `end`                   | (Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode. |
| **Example:**            | **Example:**                                                           |
| `Device(config-dial-peer)# end` |                                                                 |
### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip rsvp-fail-policy {video | voice} post-alert {optional keep-alive | mandatory {keep-alive | disconnect retry retry-attempts}} interval seconds
5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# dial-peer voice 66 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip rsvp-fail-policy {video</td>
<td>voice} post-alert {optional keep-alive</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# voice-class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 50</td>
<td>• Keywords are as follows:</td>
</tr>
<tr>
<td></td>
<td>• optional keep-alive--The keepalive messages are sent when RSVP fails only if RSVP negotiation is optional.</td>
</tr>
<tr>
<td></td>
<td>• mandatory keep-alive--The keepalive messages are sent when RSVP fails only if RSVP negotiation is mandatory.</td>
</tr>
<tr>
<td><strong>Note</strong> Keepalive messages are sent at 30-second intervals when a postalert call fails to negotiate RSVP regardless of the RSVP negotiation setting (mandatory or optional).</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>(Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring DSCP Values

Perform this task to configure different Differentiated Services Code Point (DSCP) values based on RSVP status.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `ip qos dscp {dscp-value | set-aff | set-cs | default | ef} {signaling | media [rsvp-pass | rsvp-fail] | video[rsvp-none | rsvp-pass | rsvp-fail]}`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>dial-peer voice tag voip</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# dial-peer voice 66 voip</td>
</tr>
<tr>
<td></td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip qos dscp {dscp-value</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# ip qos dscp af11 media rsvp-pass</td>
</tr>
<tr>
<td></td>
<td>Configures DSCP values based on RSVP status.</td>
</tr>
<tr>
<td></td>
<td>• Keywords are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>media rsvp-pass</strong>--Specifies that the DSCP value applies to media packets with successful RSVP reservations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>media rsvp-fail</strong>--Specifies that the DSCP value applies to packets (media or video) with failed RSVP reservations.</td>
</tr>
</tbody>
</table>
Purpose | Command or Action | Purpose
--- | --- | ---
| • The default DSCP value for all media (voice and fax) packets is ef. | • | Note: You must configure the DSCP values for all cases: media rsvp-pass and media rsvp-fail.

### Step 5

end

**Example:**

Device(config-dial-peer)# end

---

## Configuring an Application ID

Perform this task to configure a specific application ID for RSVP establishment.

### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. ip qos policy-locator {video | voice} [app app-string] [guid guid-string] [sapp subapp-string] [ver version-string]
5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
</tbody>
</table>
### Configuring Priority

Perform this task to configure priorities for call preemption.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. ip qos defending-priority defending-pri-value
5. ip qos preemption-priority preemption-pri-value
6. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>dial-peer voice tag voip</code></td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# dial-peer voice 66 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip qos defending-priority defending-pri-value</code></td>
<td>Configures the RSVP defending priority value for determining QoS.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# ip qos defending-priority 66</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip qos preemption-priority preemption-pri-value</code></td>
<td>Configures the RSVP preemption priority value for determining QoS.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# ip qos preemption-priority 75</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>(Optional) Exits dial peer configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting for Interworking Between RSVP Capable and RSVP Incapable Networks Feature**

Use the following commands to debug any errors that you may encounter when you configure the Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature.

- `debug call rsvp-sync events`
- `debug call rsvp-sync func-trace`
- `debug ccsip all`
- `debug ccsip messages`
- `debug ip rsvp messages`
- `debug sccp all`
Verifying Interworking Between RSVP Capable and RSVP Incapable Networks

This task explains how to display information to verify the configuration for the Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature. These commands need not be entered in any specific order.

SUMMARY STEPS

1. enable
2. show sip-ua calls
3. show ip rsvp installed
4. show ip rsvp reservation
5. show ip rsvp interface detail [interface-type number]
6. show sccp connections details
7. show sccp connections rsvp
8. show sccp connections internal
9. show sccp [all | connections | statistics]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show sip-ua calls</td>
<td>(Optional) Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show sip-ua calls</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show ip rsvp installed</td>
<td>(Optional) Displays RSVP-related installed filters and corresponding bandwidth information.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show ip rsvp installed</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show ip rsvp reservation</td>
<td>(Optional) Displays RSVP-related receiver information currently in the database.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show ip rsvp reservation</td>
<td></td>
</tr>
</tbody>
</table>
### Feature Information for Interworking Between RSVP Capable and RSVP Incapable Networks

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

Feature History Table entry for the Cisco Unified Border Element.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip rsvp interface detail [interface-type number]</td>
<td>(Optional) Displays the interface configuration for hello.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet 0/0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sccp connections details</td>
<td>(Optional) Displays SCCP connection details, such as call-leg details.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# show sccp connections details</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sccp connections rsvp</td>
<td>(Optional) Displays information about active SCCP connections that are using RSVP.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# show sccp connections rsvp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sccp connections internal</td>
<td>(Optional) Displays the internal SCCP details, such as time-stamp values.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# show sccp connections internal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sccp [all</td>
<td>connections</td>
<td>statistics]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# show sccp statistics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5: Feature Information for Interworking Between RSVP Capable and RSVP Incapable Networks

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interworking Between RSVP Capable and RSVP Incapable Networks</td>
<td>15.0(1)XA 15.1(1)T</td>
<td>The Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE. The following commands were introduced or modified: <code>acc-qos</code>, <code>ip qos defending-priority</code>, <code>ip qos dscp</code>, <code>ip qos policy-locator</code>, <code>ip qos preemption-priority</code>, <code>req-qos</code>, <code>voice-class sip rsvp-fail-policy</code>,</td>
</tr>
<tr>
<td>Interworking Between RSVP Capable and RSVP Incapable Networks</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>The Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE. The following commands were introduced or modified: <code>acc-qos</code>, <code>ip qos defending-priority</code>, <code>ip qos dscp</code>, <code>ip qos policy-locator</code>, <code>ip qos preemption-priority</code>, <code>req-qos</code>, <code>voice-class sip rsvp-fail-policy</code>,</td>
</tr>
</tbody>
</table>
Cisco Resource Reservation Protocol Agent

The Cisco RSVP Agent feature enables the call admission control (CAC) mechanism based on the Resource Reservation Protocol (RSVP), which is applicable to any network topology and which eases the restriction of a traditional hub-and-spoke topology.

- **Finding Feature Information**, page 49
- **Prerequisites for Cisco Resource Reservation Protocol Agent**, page 49
- **Configuring Cisco Resource Reservation Protocol Agent**, page 50
- **Feature Information for Cisco Resource Reservation Protocol Agent**, page 50

**Finding Feature Information**

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

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

**Prerequisites for Cisco Resource Reservation Protocol Agent**

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(4)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

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

To enable this feature, see the "Unified CM RSVP-Enabled Locations" section in the "Call Admission Control" chapter of the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 7.x Guide at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/cac.html#wp1043949

Detailed command information for the dspfarm profile, ip rsvp bandwidth, maximum sessions, switchover method immediate, switchback method guard timeout, and timer receiver-rtp commands are located in the Cisco IOS Voice Command Reference.

Feature Information for Cisco Resource Reservation Protocol Agent

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

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

Table 6: Feature Information for Cisco RSVP Agent

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Resource Reservation Protocol (RSVP) Agent</td>
<td>12.4(4)T</td>
<td>Enables the CAC mechanism based on the RSVP agent. The following commands were introduced or modified: dspfarm profile, ip rsvp bandwidth, maximum sessions, switchover method immediate, switchback method guard timeout, and timer receiver-rtp.</td>
</tr>
<tr>
<td>Cisco Resource Reservation Protocol (RSVP) Agent</td>
<td>Cisco IOS XE Release 3.3S</td>
<td>Enables the CAC mechanism based on the RSVP agent. The following commands were introduced or modified: dspfarm profile, ip rsvp bandwidth, maximum sessions, switchover method, and timer receiver-rtp.</td>
</tr>
</tbody>
</table>
CHAPTER 6

SIP INFO Method for DTMF Tone Generation

The SIP: INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual tone multifrequency (DTMF) tones on the telephony call leg. SIP info methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. Upon receipt of a SIP INFO message with DTMF relay content, the gateway generates the specified DTMF tone on the telephony end of the call.

- Finding Feature Information, page 51
- Prerequisites for SIP INFO Method for DTMF Tone Generation, page 51
- Restrictions for SIP INFO Methods for DTMF Tone Generation, page 52
- Information About SIP INFO Method for DTMF Tone Generation, page 52
- How to Review SIP INFO Messages, page 52
- Configuring for SIP INFO Method for DTMF Tone Generation, page 53
- Troubleshooting Tips, page 53
- Feature Information for SIP INFO Method for DTMF Tone Generation, page 54

Finding Feature Information

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

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

Prerequisites for SIP INFO Method for DTMF Tone Generation

You cannot configure, enable, or disable this feature. No configuration tasks are required to configure the SIP - INFO Method for DTMF Tone Generation feature. The feature is enabled by default.
Cisco Unified Border Element

- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

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

Restrictions for SIP INFO Methods for DTMF Tone Generation

The SIP: INFO Method for DTMF Tone Generation feature includes the following signal duration parameters:

- Minimum signal duration is 100 milliseconds (ms). If a request is received with a duration less than 100 ms, the minimum duration of 100 ms is used by default.
- Maximum signal duration is 5000 ms. If a request is received with a duration longer than 5000 ms, the maximum duration of 5000 ms is used by default.
- If no duration parameter is included in a request, the gateway defaults to a signal duration of 250 ms.

Information About SIP INFO Method for DTMF Tone Generation

The SIP: INFO Method for DTMF Tone Generation feature is always enabled, and is invoked when a SIP INFO message is received with DTMF relay content. This feature is related to the DTMF Events Through SIP Signaling feature, which allows an application to be notified about DTMF events using SIP NOTIFY messages. Together, the two features provide a mechanism to both send and receive DTMF digits along the signaling path. For more information on sending DTMF event notification using SIP NOTIFY messages, refer to the DTMF Events Through SIP Signaling feature.

How to Review SIP INFO Messages

The SIP INFO method is used by a UA to send call signaling information to another UA with which it has an established media session. The following example shows a SIP INFO message with DTMF content:

```
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
```

This sample message shows a SIP INFO message received by the gateway 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.

Configuring for SIP INFO Method for DTMF Tone Generation

You cannot configure, enable, or disable this feature. No configuration tasks are required to configure the SIP - INFO Method for DTMF Tone Generation feature. The feature is enabled by default.

Troubleshooting Tips

You can display SIP statistics, including SIP INFO method statistics, by using the `show sip-ua statistics` and `show sip-ua status` commands in privileged EXEC mode. See the following fields for SIP INFO method statistics:

- **OkInfo 0/0**, under SIP Response Statistics, Success, displays the number of successful responses to an INFO request.
- **Info 0/0**, under SIP Total Traffic Statistics, displays the number of INFO messages received and sent by the gateway.

The following is sample output from the `show sip-ua statistics` command:

```
Device# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
 Informational:
 Trying 1/1, Ringing 0/0, Forwarded 0/0, Queued 0/0, SessionProgress 0/1
 Success:
 OkInvite 0/1, OkBye 1/0, OkCancel 0/0, OkOptions 0/0, OkPrack 0/0, OkPreconditionMet 0/0
 OkSubscribe 0/0, OkNotify 0/0, OkInfo 0/0, 202Accepted 0/0
 Redirection (Inbound only):
 MultipleChoice 0, MovedPermanently 0, MovedTemporarily 0, SeeOther 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, ProxyAuthRequired 0/0, ReqTimeout 0/0, Conflict 0/0, Gone 0/0, 
 LengthRequired 0/0, ReqEntityTooLarge 0/0, ReqUnsupportedMediaType 0/0, 
 BadExtension 0/0, TempNotAvailable 0/0, CallLegNonExistent 0/0, LoopDetected 0/0, 
 TooManyHops 0/0, AddrIncomplete 0/0, Ambiguous 0/0, BusyEverywhere 0/0, 
 BadEvent 0/0
 Server Error:
 InternalError 0/0, NotImplemented 0/0, BadGateway 0/0, ServiceUnavailable 0/0, 
 GatewayTimeout 0/0, BadSipVer 0/0
 Global Failure:
 BusyEverywhere 0/0, Decline 0/0, NotExistAnywhere 0/0, NotAcceptable 0/0
 SIP Total Traffic Statistics (Inbound/Outbound)
 Invite 0/0, Ack 0/0, Bye 0/0, Cancel 0/0, Options 0/0,
```
The following is sample output from the `show sip-ua status` command:

```
Device# 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: 2 (rfc 2782)
SDP application configuration:
  Version line (v=) required
  Owner line (o=) required
  Session name line (s=) required
  Timespec line (t=) required
  Media supported: audio image
  Network types supported: IN
  Address types supported: IP4
  Transport types supported: RTP/AVP udptl
```

## Feature Information for SIP INFO Method for DTMF Tone Generation

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Table 7: Feature Information for SIP: INFO Method for DTMF Tone Generation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP: INFO Method for DTMF Tone Generation</td>
<td>12.2(11)T 12.3(2)T 12.2(8)YN 12.2(11)YV 12.2(11)T 12.2(15)T</td>
<td>The SIP: INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual-tone multifrequency (DTMF) tones on the telephony call leg. SIP methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. The following command was introduced: <code>show sip-ua</code>.</td>
</tr>
</tbody>
</table>
## Feature Information for SIP INFO Method for DTMF Tone Generation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP: INFO Method for DTMF Tone Generation</td>
<td>Cisco IOS XE Release 2.5S</td>
<td>The SIP: INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual-tone multifrequency (DTMF) tones on the telephony call leg. SIP methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. The following command was introduced: <code>show sip-ua</code>.</td>
</tr>
</tbody>
</table>
DTMF Events through SIP Signaling

The DTMF Events through SIP Signaling feature provides the following:

- DTMF event notification for SIP messages.
- Capability of receiving hookflash event notification through the SIP NOTIFY method.
- Third-party call control, or other signaling mechanisms, to provide enhanced services, such as calling card and messaging services.
- Communication with the application outside of the media connection.

The DTMF Events through SIP Signaling feature allows telephone event notifications to be sent through SIP NOTIFY messages, using the SIP SUBSCRIBE/NOTIFY method as defined in the Internet Engineering Task Force (IETF) draft, SIP-Specific Event Notification. The feature also supports sending DTMF notifications based on the IETF draft: Signaled Telephony Events in the Session Initiation Protocol (SIP) (draft-mahy-sip-signaled-digits-01.txt).

- Finding Feature Information, page 57
- Prerequisites for DTMF Events through SIP Signaling, page 58
- Restrictions for DTMF Events through SIP Signaling, page 58
- DTMF Dialing, page 58
- NOTIFY Messages, page 58
- Configuring DTMF Events through SIP Signaling, page 59
- Troubleshooting Tips, page 65
- Feature Information for DTMF Events through SIP Signaling, page 65

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Prerequisites for DTMF Events through SIP Signaling**

**Cisco Unified Border Element**

- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

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

**Restrictions for DTMF Events through SIP Signaling**

The DTMF Events through SIP Signaling feature adds support for sending telephone-event notifications via SIP NOTIFY messages from a SIP gateway. The events for which notifications are sent out are DTMF events from the local Plain Old Telephone Service (POTS) interface on the gateway. Notifications are not sent for DTMF events received in the Real-Time Transport Protocol (RTP) stream from the recipient user agent.

**DTMF Dialing**

DTMF dialing consists of simultaneous voice-band tones generated when a button is pressed on a telephone. The use of DTMF signaling for this feature enables support for advanced telephony services. Currently there are a number of application servers and service creation platforms that do not support media connections. To provide value-added services to the network, these servers and platforms need to be aware of signaling events from a specific participant in the call. Once the server or platform is aware of the DTMF events that are being signaled, it can use third-party call control, or other signaling mechanisms, to provide enhanced services. Examples of the types of services and platforms that are supported by this feature are various voice web browser services, Centrex switches or business service platforms, calling card services, and unified message servers. All of these applications require a method for the user to communicate with the application outside of the media connection. The DTMF Events Through SIP Signaling feature provides this signaling capability. This feature is related to the SIP INFO Method for DTMF Tone Generation feature, which adds support for out-of-band DTMF tone generation using the SIP INFO method. Together the two features provide a mechanism to both send and receive DTMF digits along the signaling path.

**NOTIFY Messages**

The SIP event notification mechanism uses NOTIFY messages to signal when certain telephony events take place. In order to send DTMF signals through NOTIFY messages, the gateway notifies the subscriber when DTMF digits are signaled by the originator. The notification contains a message body with a SIP response status line.
The following sample message shows a NOTIFY message from the Notifier letting the Subscriber know that the subscription is completed. The combination of the From, To, and Call-ID headers identifies the call leg. The Events header specifies the event type being signaled, and the Content-Type specifies the Internet media type. The Content-Length header indicates the number of octets in the message body.

```
NOTIFY sip:subscriber@example1.com SIP/2.0
Via: SIP/2.0/UDP example2.com:5060
From: Notifier <sip:notifier@example2.com>;tag=5678-EFGH
To: Subscriber <sip:subscriber@example1.com>;tag=1234-ABCD
Call-ID: 12345@example2.com
CSeq: 104 NOTIFY
Contact: Notifier <sip:notifier@example2.com>
Events: telephone-event;rate=1000
Content-Type: audio/telephone-event
Content-Length: 4
```

## Configuring DTMF Events through SIP Signaling

To configure the DTMF Events through SIP Signaling feature, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sip-ua`
4. `timers notify number`
5. `retry notify number`
6. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enters privileged EXEC mode or any other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>sip-ua</code></td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# sip-ua</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>timers notify number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-sip-ua)# timers notify 100</td>
</tr>
</tbody>
</table>

**Purpose**

Sets the amount of time that the user agent waits before retransmitting the Notify message. The argument is as follows:

- **number** --Time, in milliseconds, to wait before retransmitting. Range: 100 to 1000. Default: 500.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>retry notify number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-sip-ua)# retry notify 6</td>
</tr>
</tbody>
</table>

**Purpose**

Sets the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request. The argument is as follows:

- **number** --Number of retries. Range: 1 to 10. Default: 10.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-sip-ua)# exit</td>
</tr>
</tbody>
</table>

**Purpose**

Exits the current mode.

---

## Verifying SIP DTMF Support

To verify SIP DTMF support, perform the following steps as appropriate (commands are listed in alphabetical order).

### SUMMARY STEPS

1. show running-config
2. show sip-ua retry
3. show sip-ua statistics
4. show sip-ua status
5. show sip-ua timers
6. show voip rtp connections
7. show sip-ua calls

### DETAILED STEPS

**Step 1**

**show running-config**

Use this command to show dial-peer configurations.

The following sample output shows that the `dtmf-relay sip-notify` command is configured in dial peer 123:
Example:

Device# show running-config
  
  dial-peer voice 123 voip
  destination-pattern [12]...
  monitor probe icmp-ping
  session protocol sipv2
  session target ipv4:10.8.17.42
  dtmf-relay sip-notify

The following sample output shows that DTMF relay and NTE are configured on the dial peer.

Example:

Device# show running-config
  
  dial-peer voice 1000 pots
  destination-pattern 4961234
  port 1/0/0
  
  dial-peer voice 2000 voip
  application session
  destination-pattern 4965678
  session protocol sipv2
  session target ipv4:192.0.2.34
  dtmf-relay rtp-nte
  ! RTP payload type value = 101 (default)
  
  dial-peer voice 3000 voip
  application session
  destination-pattern 2021010101
  session protocol sipv2
  session target ipv4:192.0.2.34
  dtmf-relay rtp-nte
  rtp payload-type nte 110
  ! RTP payload type value = 110 (user assigned)

Step 2 show sip-ua retry
Use this command to display SIP retry statistics.

Example:

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

Step 3 show sip-ua statistics
Use this command to display response, traffic, and retry SIP statistics.

Tip To reset counters for the show sip-ua statistics display, use the clear sip-ua statistics command.

Example:

Device# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Following is sample output verifying configuration of the SIP INFO Method for DTMF Tone Generation feature:

Example:

Device# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
  Informational: Trying 1/1, Ringing 0/0,
  Forwarded 0/0, Queued 0/0,
  SessionProgress 0/1
  Success: OkInvite 0/1, OkBye 0/1,
  OkCancel 0/0, OkOptions 0/0,
  OkPrack 0/0, OkPreconditionMet 0/0,
  OkNotify 0/0, 202Accepted 0/0
  Redirection (Inbound only): MultipleChoice 0, MovedPermanently 0,
  MovedTemporarily 0, SeeOther 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,
  LengthRequired 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, RequestReset 0/0
  Server Error: InternalError 0/1, NotImplemented 0/0,
  BadGateway 0/0, ServiceUnavai 0/0,
  GatewayTimeout 0/0, BadSipVer 0/0,
  PreConFailure 0/0
  Global Failure: BusyEverywhere 0/0, Decline 0/0,
  NotExistAnywhere 0/0, NoAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound) /* Traffic Statistics
  Invite 3/2, Ack 3/2, Bye 1/0,
  Cancel 0/1, Options 0/0,
  Prack 0/2, Comet 0/0,
  Notify 0/1, Refer 1/0
Retry Statistics /* Retry Statistics
  Invite 0, Bye 0, Cancel 0, Response 0,
  Prack 0, Comet 0, Reliable1xx 0, Notify 0
DTMF Events through SIP Signaling

Verifying SIP DTMF Support

LengthRequired 0/0, ReqEntityTooLarge 0/0, ReqURITooLarge 0/0, UnsupportedMediaType 0/0, BadExtension 0/0, TempNotAvailable 0/0, CallLegNonExistsent 0/0, LoopDetected 0/0, TooManyHops 0/0, AddrIncomplete 0/0, Ambiguous 0/0, BusyHere 0/0, BadEvent 0/0

Server Error:
InternalError 0/0, NotImplemented 0/0, BadGateway 0/0, ServiceUnavailable 0/0, GatewayTimeout 0/0, BadSipVer 0/0

Global Failure:
BusyEverywhere 0/0, Decline 0/0, NotExistAnywhere 0/0, NotAcceptable 0/0

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

Retry Statistics
  Invite 0, Bye 0, Cancel 0, Response 0, Notify 0

Step 4

show sip-ua status

Use this command to display status for the SIP user agent.

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 bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
SDP application configuration:
  Version line (v=) required
  Owner line (o=) required
  Session name line (s=) required
  Timespec line (t=) required
  Media supported: audio image
  Network types supported: IN
  Address types supported: IP4
  Transport types supported: RTP/AVP udptl

The following sample output shows that the time interval between consecutive NOTIFY messages for a telephone event is the default of 2000 ms:

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 bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 6
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
SDP application configuration:
Version line (v=) required
Owner line (o=) required
Timespec line (t=) required
Media supported: audio image
Network types supported: IN
Address types supported: IP4
Transport types supported: RTP/AVP udptl

The following sample output shows configuration of the SIP INFO Method for DTMF Tone Generation feature:

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 bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
SDP application configuration:
Version line (v=) required
Owner line (o=) required
Session name line (s=) required
Timespec line (t=) required
Media supported: audio image
Network types supported: IN
Address types supported: IP4
Transport types supported: RTP/AVP udptl
```

**Step 5**

**show sip-ua timers**

Use this command to display the current settings for SIP user-agent timers.

Example:

```
Device# show sip-ua timers
SIP UA Timer Values (millsecs)
trying 500, expires 300000, connect 500, disconnect 500
comet 500, prack 500, rel1xx 500, notify 500
```

**Step 6**

**show voip rtp connections**

Use this command to show local and remote Calling ID and IP address and port information.

**Step 7**

**show sip-ua calls**

Use this command to ensure the DTMF method is SIP-KPML.

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-b4f95b6ad172.18.193.251
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 
Called Number : 8888
Bit Flags : 0x0d4018 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

Troubleshooting Tips

- To enable debugging for RTP named-event packets, use the `debug voip rtp` command.
- To enable KPML debugs, use the `debug kpml` command.
- To enable SIP debugs, use the `debug ccsip` command.
- Collect debugs while the call is being established and during digit presses.
- If an established call is not sending digits through KPML, use the `show sip-ua calls` command to ensure SIP-KPML is included in the negotiation process.

Feature Information for DTMF Events through SIP Signaling

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 8: Feature Information for Configuring DTMF Events through SIP Signaling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTMF Events through SIP Signaling</td>
<td>12.2(11)T 12.2(8)YN</td>
<td>The DTMF Events</td>
</tr>
<tr>
<td></td>
<td>12.2(15)T 12.2(11)YV</td>
<td>through SIP</td>
</tr>
<tr>
<td></td>
<td>12.2(11)T</td>
<td>Signaling feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provides the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DTMF event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notification for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIP messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Capability of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>receiving hookflash</td>
</tr>
<tr>
<td></td>
<td></td>
<td>event notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through the SIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTIFY method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Third-party call</td>
</tr>
<tr>
<td></td>
<td></td>
<td>control, or other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>signaling mechanisms,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to provide enhanced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>services, such as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>calling card and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>messaging services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Communication with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>outside of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>media connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following</td>
</tr>
<tr>
<td></td>
<td></td>
<td>commands were</td>
</tr>
<tr>
<td></td>
<td></td>
<td>introduced or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>modified: timers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notify and retry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notify.</td>
</tr>
<tr>
<td>DTMF Events through SIP Signaling</td>
<td>Cisco IOS XE Release 2.5</td>
<td>The DTMF Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through SIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signaling feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>provides the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DTMF event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notification for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIP messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Capability of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>receiving hookflash</td>
</tr>
<tr>
<td></td>
<td></td>
<td>event notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through the SIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTIFY method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Third-party call</td>
</tr>
<tr>
<td></td>
<td></td>
<td>control, or other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>signaling mechanisms,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to provide enhanced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>services, such as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>calling card and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>messaging services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Communication with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>outside of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>media connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following</td>
</tr>
<tr>
<td></td>
<td></td>
<td>commands were</td>
</tr>
<tr>
<td></td>
<td></td>
<td>introduced or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>modified: timers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notify and retry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>notify.</td>
</tr>
</tbody>
</table>
CHAPTER 8

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 (Cisco UBE), and digital signal processors (DSP) perform the CPA functionality.

- Feature Information for Call Progress Analysis Over IP-IP Media Session, page 69
- Restrictions for Call Progress Analysis Over IP-to-IP Media Session, page 70
- Information About Call Progress Analysis Over IP-IP Media Session, page 71
- How to Configure Call Progress Analysis Over IP-to-IP Media Session, page 72
- Configuration Examples for the Call Progress Analysis Over IP-to-IP Media Session, page 75

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 9: Feature Information for Call Progress Analysis Over IP-IP Media Session

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Progress Analysis Over IP-to-IP Media Session</td>
<td>15.3(2)T</td>
<td>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: <code>call-progress-analysis</code>.</td>
</tr>
<tr>
<td>Call Progress Analysis Over IP-to-IP Media Session</td>
<td>Cisco IOS XE Release 3.9S</td>
<td>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: <code>call-progress-analysis</code>.</td>
</tr>
<tr>
<td>Support for additional call flows</td>
<td>15.5(2)T Cisco IOS XE Release 3.15S</td>
<td>Call Progress Analysis feature is enhanced to support the following call-flows: • 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</td>
</tr>
</tbody>
</table>

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 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.

Information About Call Progress Analysis Over IP-IP Media Session

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 Cisco Unified Border Element (Cisco UBE).

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 Cisco UBE. The Cisco UBE 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 10: X-cisco-cpa content meaning

<table>
<thead>
<tr>
<th>SIP Message</th>
<th>Direction of Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>18x or 200</td>
<td>Cisco IOS to dialer</td>
<td>Cisco UBE informs the dialer if CPA is enabled for a call or not.</td>
</tr>
<tr>
<td>New INVITE</td>
<td>Dialer to Cisco IOS</td>
<td>Dialer requests Cisco IOS or the Cisco UBE to activate the CPA algorithm for this session.</td>
</tr>
<tr>
<td>UPDATE</td>
<td>Cisco IOS to dialer</td>
<td>Cisco IOS or the Cisco UBE notifies the dialer about the detected event.</td>
</tr>
</tbody>
</table>

CPA Events

Table 11: CPA Event Detection List

<table>
<thead>
<tr>
<th>CPA Event</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asm</td>
<td>Answer machine</td>
</tr>
</tbody>
</table>
How to Configure Call Progress Analysis Over IP-to-IP Media Session

Enabling 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| **Example:** Device> enable |  
| | • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
| **Example:** Device# configure terminal | |
| **Step 3** dspfarm profile profile-identifier transcode | Enters DSP farm profile configuration mode, defines a profile for DSP farm services, and enables the profile for transcoding.  
| **Example:** Device(config)# dspfarm profile 15 transcode | |
| **Step 4** call-progress-analysis | Enables call progress analysis (CPA) on Cisco UBE.  
| **Example:** Device(config-dspfarm-profile)# call-progress-analysis | • You must configure this command to activate the CPA feature and set CPA parameters. |
| **Step 5** exit | Exits DSP farm profile configuration mode and enters global configuration mode.  
| **Example:** Device(config-dspfarm-profile)# exit | |
| **Step 6** voice service voip | Enters voice service configuration mode.  
| **Example:** Device(config)# voice service voip | |
| **Step 7** cpa timing live-person max-duration | (Optional) Sets the maximum waiting time (in milliseconds) that the CPA algorithm uses to determine if a call is answered by a live human.  
| **Example:** Device(conf-voi-serv)# cpa timing live-person 2501 | |
| **Step 8** cpa timing term-tone max-duration | (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.  
| **Example:** Device(conf-voi-serv)# cpa timing term-tone 15500 | |
### Purpose

Command or Action | Purpose
--- | ---
**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.  
- 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.

### Verifying 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
Troubleshooting Tips

Use the following commands to troubleshoot the call progress analysis for SIP-to-SIP calls:

- `debug csip all`
- `debug voip ecapi inout`
- `debug voip hpi all`
- `debug voip ipipgw`
- `debug voip media resource provisioning all`

Configuration Examples for the Call Progress Analysis Over IP-to-IP Media Session

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
```
Example: Enabling CPA and Setting the CPA Parameters
Codec Preference Lists

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 CUBE to send an outgoing offer with all configured audio codecs in the list assuming that the dspfarm supports all these codecs.

- Feature Information for Negotiation of an Audio Codec from a List of Codecs, page 77
- Codecs configured using Preference Lists, page 78
- Prerequisites for Codec Preference Lists, page 79
- Restrictions for Codecs Preference Lists, page 79
- How to Configure Codec Preference Lists, page 80
- Troubleshooting Negotiation of an Audio Codec from a List of Codecs, page 83
- Verifying Negotiation of an Audio Codec from a List of Codecs, page 83

Feature Information for Negotiation of an Audio Codec from a List of Codecs

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 12: 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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>15.1(2)T</td>
<td>The 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 supports negotiation of an audio codec using the Voice Class Codec and Codec Transparent infrastructure on the Cisco UBE. The following command was introduced or modified: <code>voice-class codec (dial peer)</code>.</td>
</tr>
<tr>
<td>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</td>
<td>Cisco IOS XE Release 3.8S</td>
<td>The 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 supports negotiation of an audio codec using the Voice Class Codec and Codec Transparent infrastructure on the Cisco UBE. The following command was introduced or modified: <code>voice-class codec (dial peer)</code>.</td>
</tr>
<tr>
<td>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.</td>
<td>15.3(2)T</td>
<td>This feature provides high availability support 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 under the Voice Class Codec.</td>
</tr>
</tbody>
</table>

Codec Preference Lists

SIP-to-SIP calls configured using codecs using preference lists have the following features:

- Incoming and outgoing dial-peers can be configured with different preference lists.
- Both normal transcoding and high-density transcoding are supported with preference lists.
- Mid-call codec changes for supplementary services are supported with preference lists. Transcoder resources are dynamically inserted or deleted when required.
• Reinvite-based supplementary services 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 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 mid-call renegotiation, if the call releases the transcoder, then the call is checkpointed.

Prerequisites for Codec Preference Lists

• Transcoding configuration on the CUBE.

• The digital signal processor (DSP) requirements to support the transcoding feature on the CUBE.

Restrictions for Codecs Preference Lists

For All Calls (SIP-to-SIP, H323-to-H323, SIP-to-H323 calls)

• Video codecs are not supported with preference lists.

• Multiple audio streams are not supported.

• High-density transcoding is not supported when delayed offer to early offer is configured. Only low density transcoding is supported.

• Codec re-packetization feature is not supported when preference lists are configured.

For H323-to-H323 and SIP-to-H323 Calls

The below restrictions do not exist for SIP-to-SIP calls from 15.1(2)T and Cisco IOS XE Release 3.8S onwards.

• You can configure dissimilar preference lists on the incoming and outgoing dial peers.

• Incoming and outgoing dial-peers cannot be configured with the different preference lists.

• Transcoding is not supported when preference lists are used.

• Mid-call codec changes and supplementary services (call-hold / resume, call forward) do not work when a preference list is configured.

• Mid-call insertion or deletion of transcoder is not supported with preference lists.

• Rotary dial peers are not supported when preference lists are used.

• Both incoming and outgoing dial-peers need to be configured with the same codec voice classes.

• The preference of codecs configured in a codec voice classes is not be applied to the outgoing call-leg. Basically codec filtering is applied first and only the filtered codecs will be sent out in the outgoing offer from CUBE.
• T.38 fax, fax-passthru and modem-passthru is not be supported with preference lists.
• SRTP<->RTP is not supported with preference lists.
• When a codec voice class is configured, call establishment is un-predictable when a transcoder is involved in the call. The call succeeds only if the end points choose the first codec in the list of offered codecs.

How to Configure Codec Preference Lists

Configuring 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[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 offer-all
8. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
|        | Example:  
Device> enable | • Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode. |
|        | Example:  
Device> configure terminal | |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters voice-class configuration mode for the specified codec voice class.</td>
</tr>
<tr>
<td>voice class codec tag</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# voice class codec 10</td>
</tr>
</tbody>
</table>

**Step 4**
Do the following for each audio codec you want to configure in the voice class:

- 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 specifies a preference for the codec. This becomes part of a preference list.

**Step 5**
Exits the current mode.
- **exit**

**Example:**
Device(config-class)# exit

**Step 6**
Enter dial peer configuration mode for the specified VoIP dial peer.
- dial-peer voice number voip

**Example:**
Device(config)# dial-peer voice 1 voip

**Step 7**
Applies the previously configured voice class and associated codecs to a dial peer.
- voice-class codec tag offer-all

**Example:**
Device(config-dial-peer)# voice-class codec 10

- The **offer-all** keyword allows the device to offer all codecs configured in a codec voice class.

**Step 8**
Returns to privileged EXEC mode.
- **end**

**Example:**
Device(config-dial-peer)# end

---

**Disabling Codec Filtering**

Cisco UBE is configured to filter common codecs for the subsets, by default. The filtered codecs are sent in the outgoing offer. You can configure the Cisco UBE to offer all the codecs configured on an outbound leg instead of offering only the filtered codecs.
This configuration is applicable only for early offer calls from the Cisco UBE. 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>dial-peer voice <em>tag</em> voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# dial-peer voice 10 voip</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>voice-class codec <em>tag</em> offer-all</td>
<td>Adds all the configured voice class codec to the outgoing offer from the Cisco UBE.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# voice-class codec 10 offer-all</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting 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 Cisco Unified Border Element feature:

- debug ccsip all
- debug voip ccapi input
- debug sccp messages
- 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

Verifying 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 sccp connections
5. 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
Verifying Negotiation of an Audio Codec from a List of Codecs

Codec Preference Lists

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 3 14 18422 2000 192.0.2.4
9.44.26.3
4 15 14 16576 2000 192.0.2.5
192.0.2.6
```

Cisco Unified Border Element (Enterprise) Protocol-Independent Features and Setup Configuration Guide,
Cisco IOS XE Release 3S
Step 4  **show sccp connections**  
Displays information about the connections controlled by the Skinny Client Control Protocol (SCCP) transcoding and conferencing applications.

**Example:**

```
Device# show sccp connections
sess_id conn_id stype mode codec sport rport ripaddr
5  5  xcode sendrecv g729b 16576 2000 192.0.2.3
5  6  xcode sendrecv g711u 18422 2000 192.0.2.4
```

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

Step 5  **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 DSFPARM DSP channel(s) 1
Verifying Negotiation of an Audio Codec from a List of Codecs
The AAC-LD MP4A-LATM codec is a wideband audio codec used by video endpoints. MP4A-LATM is an MPEG4 audio coding standard, where LATM is Low-Overhead MPEG-4 Audio Transport Multiplex. The Cisco Unified Border Element (Cisco UBE) supports MP4A-LATM to enable call flows involving endpoints that use this codec, especially for media recording.

For basic information on Codecs and how to configure them, refer to Codecs in the Cisco Unified Border Element Fundamentals and Basic Setup.

- Finding Feature Information, page 87
- Restrictions for AAC-LD MP4A-LATM Codec Support on Cisco UBE, page 88
- AAC-LD MP4A-LATM Codec Support on Cisco UBE, page 88
- How to Configure the MP4A-LATM Codec, page 89
- Configuration Examples for AAC-LD MP4A-LATM Codec Support on Cisco UBE, page 93
- Feature Information for AAC-LD MP4A-LATM Codec Support on Cisco UBE, page 94

**Finding Feature Information**

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for AAC-LD MP4A-LATM Codec Support on Cisco UBE

Cisco UBE 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

AAC-LD MP4A-LATM Codec Support on Cisco UBE

As part of this feature, Cisco UBE 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 Cisco UBE 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 Cisco UBE with codec filtering
  - SRTP and SRCTP 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
  - Cisco UBE Mid-call Re-INVITE consumption
How to Configure the MP4A-LATM Codec

Configuring the MP4A-LATM Codec on a Dial Peer

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. destination-pattern [+string [T]
5. session protocol sipv2
6. session target ipv4:destination-address
7. codec mp4a-latm [profile tag]
8. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Specifies the method of voice encapsulation and enters dial peer voice configuration mode for the specified dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# dial-peer voice 24 voip</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>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:</td>
</tr>
<tr>
<td><code>destination-pattern [+ string [T]]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-dial-peer)# destination-pattern 595959</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+ --(Optional) Character that indicates an E.164 standard number.</td>
</tr>
<tr>
<td></td>
<td><code>string</code> --Series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and any special character.</td>
</tr>
<tr>
<td></td>
<td><code>T</code> --(Optional) Control character indicating that the <code>destination-pattern</code> value is a variable-length dial string.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the VoIP dial peer to use Session Initiation Protocol (SIP).</td>
</tr>
<tr>
<td><code>session protocol sipv2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-dial-peer)# session protocol sipv2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies a network-specific address for a dial peer. Keyword and argument are as follows:</td>
</tr>
<tr>
<td><code>session target ipv4:destination-address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-dial-peer)# session target ipv4:10.42.29.7</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ipv4</code>: <code>destination address</code> --IP address of the dial peer, in this format: <code>xxx.xxx.xxx.xxx</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Configures the MP4A-LATM codec for the dial peer.</td>
</tr>
<tr>
<td><code>codec mp4a-latm [profile tag]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-dial-peer)# codec mp4a-latm profile 5</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Exits dial peer voice configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config-dial-peer)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the MP4A-LATM Codec under Voice Class Codec

SUMMARY STEPS

1. enable
2. configure terminal
3. voice class codec tag
4. codec preference value codec-type [profile tag]
5. exit
6. dial-peer voice tag voip
7. destination-pattern [+] string [T]
8. session protocol sipv2
9. session target ipv4:destination-address
10. voice-class codec tag

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice class codec tag</td>
<td>Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.</td>
</tr>
<tr>
<td>Example: Device(config)# voice class codec 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> codec preference value codec-type [profile tag]</td>
<td>Specifies the preferred codec (or codecs) to use on a dial peer.</td>
</tr>
<tr>
<td>Example: Device(config-class)# codec preference 1 mp4a-latm profile 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits voice-class configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-class)# exit</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong> dial-peer voice tag voip</td>
<td>Specifies the method of voice encapsulation and enters dial peer voice configuration mode for the specified dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# dial-peer voice 24 voip</td>
</tr>
<tr>
<td><strong>Step 7</strong> destination-pattern [+ string [T]]</td>
<td>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:</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# destination-pattern 595959</td>
</tr>
<tr>
<td><strong>Step 8</strong> session protocol sipv2</td>
<td>Configures the VoIP dial peer to use Session Initiation Protocol (SIP).</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# session protocol sipv2</td>
</tr>
<tr>
<td><strong>Step 9</strong> session target ipv4:destination-address</td>
<td>Specifies a network-specific address for a dial peer. Keyword and argument are as follows:</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# session target ipv4:10.42.29.7</td>
</tr>
<tr>
<td><strong>Step 10</strong> voice-class codec tag</td>
<td>Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# voice-class codec 1</td>
</tr>
</tbody>
</table>

**Verifying an Audio Call**

**SUMMARY STEPS**

1. show call active voice [compact]
**DETAILED STEPS**

**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
  23 ANS T3 mp4a-latm VOIP Psipp 9.45.33.11:57210
  24 ORG T3 mp4a-latm VOIP P123 9.45.33.11:57210
```

```
Device# 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 P500110011 10.13.37.150:6090
```

### Configuration Examples for AAC-LD MP4A-LATM Codec Support on Cisco UBE

**Example: Configuring the MP4A-LATM Codec under a Dial Peer**

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 24 voip
Device(config-dial-peer)# destination-pattern 595959
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.42.29.7
Device(config-dial-peer)# codec mp4a-latm profile 5
Device(config-dial-peer)# end
```

**Example: Configuring the MP4A-LATM Codec under Voice Class Codec**

```
Device> enable
Device# configure terminal
Device(config)# voice class codec 1
Device(config-class)# codec preference 1 mp4a-latm profile 5
Device(config-class)# exit
Device(config)# dial-peer voice 24 voip
Device(config-dial-peer)# destination-pattern 595959
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.42.29.7
Device(config-dial-peer)# voice-class codec 1
```
Feature Information for AAC-LD MP4A-LATM Codec Support on Cisco UBE

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 13: Feature Information for AAC-LD MP4A-LATM Codec Support on Cisco UBE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC-LD MP4A-LATM Codec Support on Cisco UBE</td>
<td>Cisco IOS XE Release 3.12S</td>
<td>The AAC-LD MP4A-LATM codec is a wideband audio codec used by video endpoints. MP4A-LATM is an MPEG4 audio coding standard, where LATM is Low-Overhead MPEG-4 Audio Transport Multiplex. The Cisco Unified Border Element (Cisco UBE) supports MP4A-LATM to enable call flows involving endpoints that use this codec, especially for media recording. The following commands were introduced or modified: <code>codec mp4a-latm</code>, <code>codec preference tag mp4a-latm</code></td>
</tr>
</tbody>
</table>
Multicast Music-on-Hold Support on Cisco UBE

First Published: July 22, 2011
Last Updated: July 22, 2011

The Multicast Music-on-Hold (MMOH) feature enables you to subscribe to a music streaming service when you are using a Cisco Unified Border Element. Music streams from an MMOH server to the interface of Cisco UBE, which then converts it into unicast. To play the MMOH to customers using Cisco UBE, you must enable the MMOH feature on Cisco UBE.

- Prerequisites for Multicast Music-on-Hold Support on Cisco UBE, page 95
- Restrictions for Multicast Music-on-Hold Support on Cisco UBE, page 95
- Information About Multicast Music-on-Hold Support on Cisco UBE, page 96
- How to Enable Multicast Music-on-Hold on Cisco UBE, page 96
- Configuration Examples for Multicast Music-on-Hold Support on Cisco UBE, page 101
- Feature Information for Multicast Music-on-Hold Support on Cisco UBE, page 103

Prerequisites for Multicast Music-on-Hold Support on Cisco UBE

Cisco Unified Border Element

- Cisco IOS Release 15.2(1)T or a later release must be installed and running on your Cisco Unified Border Element.

Restrictions for Multicast Music-on-Hold Support on Cisco UBE

- The Multicast Music-on-Hold (MMOH) feature will not work when the Session Description Protocol (SDP) Passthrough feature is enabled on Cisco UBE.
• The MMOH feature will work for Low Density Transcoded calls but not for High Density Transcoded calls.
• MMOH is supported only on SIP-to-SIP call flows on Cisco UBE.
• MMOH with RTCP is not supported.
• MMOH is not supported for SRTP trunk.
• MMOH with media flow-around is not supported.

Information About Multicast Music-on-Hold Support on Cisco UBE

Multicast Music-on-Hold

To play Multicast Music-on-Hold (MMOH) to customers using Cisco UBE, you must enable the MMOH feature on Cisco UBE. When Cisco UBE receives an MMOH call, it converts the multicast address received on the inbound leg into a unicast address and sends the address on the outbound leg.

Cisco UBE uses preconfigured CLIs to "listen" for Real-Time Transport Protocol (RTP) packets that are broadcast from an MMOH server in the network and converts them to unicast. When a call is placed on hold, the MOH server streams the RTP packets to the Cisco UBE interface. This interface converts the RTP packets to unicast and relays the packets to the appropriate voice interfaces that have been placed on hold.

Note

MMOH is already supported on SIP-TDM gateways.

How to Enable Multicast Music-on-Hold on Cisco UBE

Enabling MMOH on Cisco UBE

Perform this task to enable the MMOH feature on Cisco UBE.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip multicast-routing distributed`
4. `interface gigabitethernet router-shelf/slot/port`
5. `ip address ip-address subnet-mask`
6. `ip pim dense-mode`
7. `negotiation auto`
8. `exit`
9. `ccm-manager music-on-hold`
10. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code> Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| Example:          | Device> enable  
• Enter your password if prompted. |
<p>| <strong>Step 2</strong>        | <code>configure terminal</code> Enters global configuration mode. |
| Example:          | Device# configure terminal |
| <strong>Step 3</strong>        | <code>ip multicast-routing distributed</code> Enables distributed IP multicast routing. |
| Example:          | Device(config)# ip multicast-routing distributed |
| <strong>Step 4</strong>        | <code>interface gigabitethernet router-shelf/slot/port</code> Configures a Gigabit Ethernet interface and enters interface configuration mode. |
| Example:          | Device(config)# interface gigabitethernet 0/0/0 |
| <strong>Step 5</strong>        | <code>ip address ip-address subnet-mask</code> Configures the IP address and the subnet mask on the interface. |
| Example:          | Device(config-if)# ip address 9.40.1.140 255.255.0.0 |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>ip pim dense-mode</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# ip pim dense-mode</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>negotiation auto</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# negotiation auto</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-if)# exit</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>ccm-manager music-on-hold</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# ccm-manager music-on-hold</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# exit</td>
</tr>
</tbody>
</table>

**Verifying the MMOH Support on Cisco UBE**

Perform this task to verify the MMOH support on Cisco UBE. The `show` commands can be entered in any order.

**SUMMARY STEPS**

1. enable
2. show ccm-manager music-on-hold
3. show voip rtp connections
4. show call active voice compact
5. show platform hardware qfp active feature sbc mmoh global
6. show platform hardware qfp active feature sbc mmoh group
**DETAILED STEPS**

**Step 1**

`enable`

Enables privileged EXEC mode.

**Example:**

Device> enable

**Step 2**

`show ccm-manager music-on-hold`

Displays information about all the multicast music-on-hold (MOH) sessions in the gateway at any given time.

**Example:**

Device# show ccm-manager music-on-hold
Current active multicast sessions: 1
Multicast Address  RTP port number  Packets in/out  CallId  Codec  Incoming Interface
239.1.1.1 16386  614/614  132  g711ulaw  Gi0/0

**Step 3**

`show voip rtp connections`

Displays RTP-named event packets.

**Example:**

Device# show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 20000, Ports Reserved: 101, Ports in Use: 2
Port range not configured, Min: 8000, Max: 48200
Ports Ports Ports
Media-Address Range Available Reserved In-use
Default Address-Range 20000 101 2
VoIP RTP active connections:
No. CallId dstCallId LocalRTP RmtRTP LocalIP RemoteIP
1 140 141 18792 18638 9.42.30.10 9.42.30.189
2 141 140 19256 26184 9.42.30.10 9.42.30.189
Found 2 active RTP sessions

**Step 4**

`show call active voice compact`

Displays a compact version of 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: 3
140 ANS T644 g711ulaw VOIP P10000 9.42.30.32:18638
141 ORG T644 g711ulaw VOIP P708090 9.42.30.189:26184
145 ORG T643 g711ulaw VOIP P595959 9.42.29.7:3852

**Step 5**

`show platform hardware qfp active feature sbc mmoh global`

Displays SBC multicast Music-on-Hold global statistics.
Example:

Device# show platform hardware qfp active feature sbc mmoh global

SBC multicast Music-on-Hold Global Statistics

<table>
<thead>
<tr>
<th>Total MMOH groups</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total RTP packets received</td>
<td>6311</td>
</tr>
<tr>
<td>Total RTP octects received</td>
<td>1262200</td>
</tr>
<tr>
<td>Total RTP packets replicated</td>
<td>6311</td>
</tr>
<tr>
<td>Total RTP octects replicated</td>
<td>1262200</td>
</tr>
<tr>
<td>Total RTP packets dropped</td>
<td>0</td>
</tr>
<tr>
<td>Total RTP octects dropped</td>
<td>0</td>
</tr>
</tbody>
</table>

Step 6

show platform hardware qfp active feature sbc mmoh group

Displays SBC multicast Music-on-Hold group structure.

Example:

Device# show platform hardware qfp active feature sbc mmoh group

SBC multicast Music-on-Hold group structure:

<table>
<thead>
<tr>
<th>VRF</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>239.1.1.1</td>
</tr>
<tr>
<td>Port</td>
<td>16384</td>
</tr>
<tr>
<td>Protocol</td>
<td>1</td>
</tr>
<tr>
<td>Calls in group</td>
<td>1</td>
</tr>
</tbody>
</table>

SBC MMHO group Statistics

| Total RTP packets received | 406 |
| Total RTP octects received | 81200 |
| Total RTP packets replicated | 406 |
| Total RTP octects replicated | 81200 |
| Total RTP packets dropped | 0 |
| Total RTP octects dropped | 0 |

Troubleshooting Tips

The following commands can help troubleshoot MMOH:

- `debug ccm-manager music-on-hold [ all ] [ errors ] [ events ]`
- `debug voip rtp`
- `debug ccsip all`
Configuration Examples for Multicast Music-on-Hold Support on Cisco UBE

Example: Enabling MMOH on Cisco UBE

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing distributed
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ip address 9.40.1.140 255.255.0.0
Device(config-if)# ip pim dense-mode
Device(config-if)# negotiation auto
Device(config-if)# exit
Device(config)# ccm-manager music-on-hold
Device# show running-config
Building configuration...
Current configuration : 2375 bytes
!
! Last configuration change at 11:01:36 UTC Wed Jan 5 2011
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname carbon-1
!
boot-start-marker
boot system flash usbflash0:c2951-universalk9-mz.SSA.MMOH-carbon_dev
boot-end-marker
!
!
!
!
!
no aaa new-model
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing
!
!
oip domain lookup
multilink bundle-name authenticated
!
!
!
crypto pki token default removal timeout 0
!
!
voice-card 0
!
!
voice service voip
 mode border-element license capacity 1200
allow-connections sip to sip
sip

```
Example: Enabling MMOH on Cisco UBE

```
license udi pid CISCO2951/K9 sn FHK1433F39H
hw-module pvdm 0/0

redundancy inter-device

redundancy

interface GigabitEthernet0/0
  ip address 9.42.30.12 255.255.0.0
duplex auto
  speed auto

interface GigabitEthernet0/1
  no ip address
  shutdown
duplex auto
  speed auto

interface GigabitEthernet0/2
  no ip address
  shutdown
duplex auto
  speed auto
  ip forward-protocol nd
  no ip http server
  no ip http secure-server
  ip route 0.0.0.0 0.0.0.0 9.42.0.1
  nls resp-timeout 1
cpd cr-id 1
  control-plane

ccm-manager music-on-hold

mgcp profile default

dial-peer voice 100 voip
  destination-pattern 878767
  session protocol sipv2
  session target ipv4:9.42.30.5
  codec g711ulaw
gatekeeper
  shutdown

line con 0
  speed 115200
line aux 0
line vty 0 4
```
Feature Information for Multicast Music-on-Hold Support on Cisco UBE

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 14: Feature Information for Multicast Music-on-Hold Support on Cisco UBE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Music-on-Hold Support on Cisco UBE</td>
<td>15.2(1)T Cisco IOS XE Release 3.11S</td>
<td>The Multicast Music-on-Hold (MMOH) feature enables you to subscribe to a music streaming service when you are using a Cisco Unified Border Element. To play MMOH to customers using Cisco UBE, you must enable the MMOH feature on Cisco UBE. No new commands were introduced or modified.</td>
</tr>
</tbody>
</table>
Network-Based Recording

The Network-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 for Network-Based Recording, page 105
- Restrictions for Network-Based Recording, page 106
- Information About Network-Based Recording Using CUBE, page 107
- How to Configure Network-Based Recording, page 112
- Additional References for Network-Based Recording, page 131

Feature Information for Network-Based Recording

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 15: Feature Information for Network-Based Recording

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio-only Stream Forking of Video Call</td>
<td>Cisco IOS 15.4(3)M Cisco IOS XE 3.13S</td>
<td>The Audio-only Stream Forking of Video Call feature supports CUBE-based forking and recording of only audio calls in a call that includes both audio and video. The following commands were introduced: <code>media-type audio</code>.</td>
</tr>
<tr>
<td>Network-Based Recording of Video Calls Using CUBE</td>
<td>Cisco IOS 15.3(3)M Cisco IOS XE 3.10S</td>
<td>The Network-Based Recording of Video Calls using CUBE feature supports forking and recording of video calls.</td>
</tr>
<tr>
<td>Network-Based Recording of Audio Calls Using CUBE</td>
<td>Cisco IOS 15.2(1)T Cisco IOS XE 3.8S</td>
<td>The Network-Based Recording of Audio Calls using CUBE feature supports forking for RTP streams. The following commands were introduced or modified: <code>media class</code>, <code>media profile recorder</code>, <code>media-recording</code>, <code>recorder parameter</code>, <code>recorder profile</code>, <code>show voip recmsp session</code>.</td>
</tr>
</tbody>
</table>

Restrictions for Network-Based Recording

- Network-based recording is not supported for the following calls:
  - Calls that are not Session Initiation Protocol (SIP) SIP-to-SIP
  - 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.

• Media service parameter change via Re-INVITE or UPDATE message from the recording server is not supported.

• Recording is not supported if CUBE is running a TCL IVR application.

• Media mixing on forked streams 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.

Information About Network-Based Recording Using CUBE

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.

Given below is a typical deployment scenario of a CUBE-based recording solution. The information flow is described below:

Figure 2: Deployment Scenario for CUBE-based Recording Solution
1. Incoming call from SIP trunk.
2. Outbound call to a Contact Centre
3. Media between endpoints flow through 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 an 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.
# How to Configure Network-Based Recording

## Configuring Network-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** *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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> media profile recorder <em>profile-tag</em></td>
<td>Configures the media profile recorder and enters media profile configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# media profile recorder 100</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Network-Based Recording (with Media Profile Recorder)

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> media-type audio</td>
<td>(Optional) 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.</td>
</tr>
<tr>
<td>Example: Device(cfg-mediaprofile)# media-type audio</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> media-recording dial-peer-tag [dial-peer-tag2...dial-peer-tag5]</td>
<td>Configures the dial-peers that need to be configured. Note: You can specify a maximum of five dial-peer tags.</td>
</tr>
<tr>
<td>Example: Device(cfg-mediaprofile)# media-recording 8000 8001 8002</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits media profile configuration mode.</td>
</tr>
<tr>
<td>Example: Device(cfg-mediaprofile)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> media class tag</td>
<td>Configures a media class and enters media class configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# media class 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> recorder profile tag</td>
<td>Configures the media profile recorder.</td>
</tr>
<tr>
<td>Example: Device(cfg-mediaclass)# recorder profile 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Exits media class configuration mode.</td>
</tr>
<tr>
<td>Example: Device(cfg-mediaclass)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> dial-peer voice dummy-recorder-dial-peer-tag voip</td>
<td>Configures a recorder dial peer and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# dial-peer voice 8000 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> media-class tag</td>
<td>Configures media class on a dial peer.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# media-class 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> destination-pattern [+] string [T]</td>
<td>Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# destination-pattern 595959</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **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  
**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:  
- **ipv4**: *destination address* --IP address of the dial peer, in this format: xxx.xxx.xxx.xxx  
- **ipv4**: *recording-server-dns*  
- **ipv4**: *recording-server-destination-address* |
| **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:**  
Device(config-dial-peer)# end | Returns to privileged EXEC mode. |
Configuring Network-Based 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 media class tag</td>
<td>Configures the media class and enters media class configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# media class 100</td>
<td></td>
</tr>
<tr>
<td>Step 4 recorder parameter</td>
<td>Enters media class recorder parameter configuration mode to enable you to configure recorder-specific parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(cfg-mediaclass)# recorder parameter</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td>media-type audio</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(cfg-mediaprofile)# media-type audio</td>
</tr>
<tr>
<td>Step 6</td>
<td>media-recording <strong>dial-peer-tag</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(cfg-mediaclass-recorder)# media-recording 8000, 8001, 8002</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(cfg-mediaclass-recorder)# exit</td>
</tr>
<tr>
<td>Step 8</td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(cfg-mediaclass)# exit</td>
</tr>
<tr>
<td>Step 9</td>
<td>dial-peer <strong>voice</strong> dummy-recorder-dial-peer-tag <strong>voip</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# dial-peer voice 8000 voip</td>
</tr>
<tr>
<td>Step 10</td>
<td>media-class <strong>tag</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-dial-peer)# media-class 100</td>
</tr>
<tr>
<td>Step 11</td>
<td>destination-pattern [*] <strong>string</strong> [T]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-dial-peer)# destination-pattern 595959</td>
</tr>
<tr>
<td>Step 12</td>
<td>session protocol <strong>sipv2</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-dial-peer)# session protocol sipv2</td>
</tr>
<tr>
<td>Step 13</td>
<td>session target <strong>ipv4:</strong>[recording-server-destination-address</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# session target</td>
<td><strong>• ipv4:</strong> destination address --IP address of the dial peer, in this format: xxx.xxx.xxx.xxx</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 14</td>
<td>session transport tcp</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# session transport tcp</td>
<td></td>
</tr>
<tr>
<td>Step 15</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the Network-Based Recording Using CUBE

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 ccap 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

<table>
<thead>
<tr>
<th>Media-Address Range</th>
<th>Available</th>
<th>Reserved</th>
<th>In-use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Address-Range</td>
<td>8091</td>
<td>101</td>
<td>8</td>
</tr>
</tbody>
</table>

VoIP RTP active connections:
<table>
<thead>
<tr>
<th>No.</th>
<th>CallID</th>
<th>dstCallID</th>
<th>LocalRTP</th>
<th>RmtRTP</th>
<th>LocalIP</th>
<th>RemoteIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>16384</td>
<td>20918</td>
<td>10.104.45.191</td>
<td>10.104.8.94</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>16386</td>
<td>17412</td>
<td>10.104.45.191</td>
<td>10.104.8.98</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>16388</td>
<td>29652</td>
<td>10.104.45.191</td>
<td>10.104.8.98</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>16390</td>
<td>20036</td>
<td>10.104.45.191</td>
<td>10.104.8.94</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>5</td>
<td>16392</td>
<td>58368</td>
<td>10.104.45.191</td>
<td>10.104.105.232</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>5</td>
<td>16394</td>
<td>53828</td>
<td>10.104.45.191</td>
<td>10.104.105.232</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>5</td>
<td>16396</td>
<td>39318</td>
<td>10.104.45.191</td>
<td>10.104.105.232</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>5</td>
<td>16398</td>
<td>41114</td>
<td>10.104.45.191</td>
<td>10.104.105.232</td>
</tr>
</tbody>
</table>

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 : 7C5946D8ECD
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

<table>
<thead>
<tr>
<th>Output Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream State</td>
<td>Displays the state of the call. This can be ACTIVE or HOLD.</td>
</tr>
</tbody>
</table>
### Output Field | Description
---|---
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.

### 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
    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
    packets sent 29686, packets received 0
  stream type video (6): count 0
  stream type video (7): count
```
### Output Field
<table>
<thead>
<tr>
<th>Output Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>codec g711ulaw</td>
<td>Codec negotiated for the recording leg.</td>
</tr>
</tbody>
</table>

## 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:3, User Agent Client:2, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID : 99EA5118-506211E0-80C6E018-4C27AA62@10.42.30.10
  State of the call : STATE_ACTIVE (7)
  Substate of the call : SUBSTATE_NONE (0)
  Calling Number : 10000
  Called Number : 708090
  Bit Flags : 0xC04018 0x10000100 0x80
  CC Call ID : 141
  Source IP Address (Sig ) : 10.42.30.10
  Destn SIP Reg Addr:Port : [10.42.30.5]:5060
  Destn SIP Resp Addr:Port: [10.42.30.5]:5060
  Destination Name : 10.42.30.5
  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 : 141
    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: [10.42.30.10]:19256
Media Dest IP Addr:Port: [10.42.30.189]:26184
Options-PMG ENABLED: NO ACTIVE: NO

Call 2
SIP Call ID: 9A6D8922-506211E0-80CEEE01B-4C27AA62@10.42.30.10
State of the call: STATE_ACTIVE (7)
Substate of the call: SUBSTATE_NONE (0)
Calling Number: 595959
Called Number: 10.42.30.10
Bit Flags: 0xC04018 0x10800100 0x80
CC Call ID: 145
Source IP Address (Sig): 10.42.30.10
Destn SIP Req Addr:Port: [10.42.29.7]:5060
Destn SIP Resp Addr:Port: [10.42.29.7]:5060
Destination Name: 10.42.29.7
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: 145
Stream Type: voice-nearend (3)
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: [10.42.30.10]:18648
Media Dest IP Addr:Port: [10.42.29.7]:38526

Media Stream 2
State of the stream: STREAM_ACTIVE
Stream Call ID: 146
Stream Type: voice-farend (5)
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: [10.42.30.10]:17780
Media Dest IP Addr:Port: [10.42.29.7]:50482

SIP UAS CALL INFO
Call 1
SIP Call ID: 7CF44DF3-506611E0-8ED2B9D4-CA68C314@10.42.30.32
State of the call: STATE_ACTIVE (7)
Substate of the call: SUBSTATE_NONE (0)
Called Number: 10000
Called Number: 708090
Bit Flags: 0x8C4401C 0x10000100 0x4
CC Call ID: 140
Source IP Address (Sig): 10.42.30.10
Destn SIP Req Addr:Port: [10.42.30.32]:5060
Destn SIP Resp Addr:Port: [10.42.30.32]:52757
Destination Name: 10.42.30.32
Number of Media Streams: 1
RTP Fork Object: 0x0
Media Mode: flow-through

Media Stream 1
State of the stream: STREAM_ACTIVE
Stream Call ID: 140
Stream Type: voice+dtmf (0)
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: [10.42.30.10]:18792
Media Dest IP Addr:Port: [10.42.30.32]:18638
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

Step 10
debug ccsip messages (for audio calls)
Sent:
INVITE sip:22222@10.42.30.32:5060 SIP/2.0
Via: SIP/2.0/TCP 10.42.30.10:5060;branch=z9hG4bKt622CF
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:59595@10.42.30.32>
Supported: 100rel,timer,resource-priority, replaces,sdp-anat
Min-SE: 1800
Cisco-Guid: 1334370502-1348997600-2396699902-3395863316

IOS XE Release 3S
Network-Based Recording
Verifying the Network-Based Recording Using CUBE
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
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0
<table>
<thead>
<tr>
<th>Output Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE sip:22222@10.42.29.7:5060 SIP/2.0</td>
<td>22222 is the destination pattern or the number of recording server and is configured under the recorder dial peer.</td>
</tr>
<tr>
<td>X-Cisco-Recording-Participant: sip:708090@10.42.30.5;media-index=&quot;0&quot;</td>
<td>Cisco proprietary header with originating and terminating participant number and IP address used to communicate to the recording server</td>
</tr>
<tr>
<td>Cisco-Guid: 1334370502-1348997600-2396699092-3395863316</td>
<td>GUID is the same for the primary call and forked call.</td>
</tr>
<tr>
<td>m=audio 24544 RTP/AVP 0 101 19</td>
<td>First m-line of participant with payload type and codec information.</td>
</tr>
<tr>
<td>m=audio 31166 RTP/AVP 0 101 19</td>
<td>Second m-line of another participant with codec info and payload type.</td>
</tr>
<tr>
<td>a=sendonly</td>
<td>CUBE is always in send only mode towards Recording server.</td>
</tr>
<tr>
<td>a=recvonly</td>
<td>Recording server is in receive mode only.</td>
</tr>
</tbody>
</table>

**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
```

m=video 17236 RTP/AVP 126
```
```
Verifying the Network-Based Recording Using CUBE

<table>
<thead>
<tr>
<th>Output Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent: INVITE sip:575757@9.45.38.39:7686 SIP/2.0</td>
<td>22222 is the destination pattern or the number of recording server and is configured under the recorder dial peer.</td>
</tr>
<tr>
<td>X-Cisco-Recording-Participant: sip:1777@10.104.45.207;media-index=&quot;0 2&quot;</td>
<td>Cisco proprietary header with originating and terminating participant number and IP address used to communicate to the recording server</td>
</tr>
<tr>
<td>X-Cisco-Recording-Participant: sip:1888@10.104.45.207;media-index=&quot;1 3&quot;</td>
<td></td>
</tr>
<tr>
<td>Cisco-Guid: 0884935168-0000065536-0000000401-3475859466</td>
<td>GUID is the same for the primary call and forked call.</td>
</tr>
<tr>
<td>m=audio 17232 RTP/AVP 0 19</td>
<td>First m-line of participant with payload type and audio codec.</td>
</tr>
<tr>
<td>m=audio 17234 RTP/AVP 0 19</td>
<td>Second m-line of another participant with payload type and audio codec.</td>
</tr>
<tr>
<td>m=video 17236 RTP/AVP 126</td>
<td>Third m-line of participant with video payload type and codec info.</td>
</tr>
<tr>
<td>m=video 17238 RTP/AVP 126</td>
<td>Fourth m-line of another participant with video payload type and codec info.</td>
</tr>
<tr>
<td>a=sendonly</td>
<td>CUBE is always in send only mode towards Recording server.</td>
</tr>
</tbody>
</table>

Receive:
SIP/2.0 200 OK

m=audio 1592 RTP/AVP 0

m=audio 1594 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-FFFFFFFF8FC011E2-FFFFFFFF824DF469-FFFFFFFFB6661C0689.41.36.41
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

<table>
<thead>
<tr>
<th>Output Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>m=audio 1592 RTP/AVP 0</td>
<td>First m-line of recording server after it started listening.</td>
</tr>
<tr>
<td>m=audio 1594 RTP/AVP 0</td>
<td>Second m-line of recording server after it started listening.</td>
</tr>
<tr>
<td>m=video 1596 RTP/AVP 126</td>
<td>Third m-line of recording server after it started listening.</td>
</tr>
<tr>
<td>m=video 1598 RTP/AVP 126</td>
<td>Fourth m-line of recording server after it started listening.</td>
</tr>
<tr>
<td>a=recvonly</td>
<td>Recording server in receive only mode.</td>
</tr>
</tbody>
</table>

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
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

Step 13 Enter one of the following:

- debug csip all
- debug voip recmsp all
- debug voip ccap all
- debug voip fpi all (for ASR devices only)

Displays detailed debug messages.

For Audio:
Media forking initialized:


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:
Forking header populated:


Media forking setup record session is successful:

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: dtmf is inband
Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF: First element..
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/Info/ccsip_get_recording_participant_header: MF: Host = 9.42.30.34
Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_get_recording_participant_header: MF: Host = 9.42.30.34

Media forking forked stream started:

Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_forked_leg_config: MF: Overwriting the GUID with the value got from MSP.
Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_forked_leg_config: MF: Overwriting the GUID with the value got from MSP.

Forced stream added.

Jun 15 10:37:55.404: //103/3E7E90AE8006/SIP/Info/ccsip_ipip_media_forking_Display_TDContainerData:

** DISPLAY REC PART **
Verifying the Network-Based Recording Using CUBE

For Video:

**Media Forking Initialized:**


**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/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/33792/ccsip_get_recording_participant_header: MF: X-Cisco header is PAI.

**Recording participant for anchor leg:**


*Mar 19 16:40:01.788 IST: //522/34BF0A000000/SIP/Info/verbose/32768/ccsip_ipip_media_forking_BuildMediaRecParticipant: MF: X-Cisco header is PAI.

**Adding an audio stream:**

*Mar 19 16:40:01.788 IST: //522/34BF0A000000/SIP/Function/sipSPIGetFirstStream:


*Mar 19 16:40:01.789 IST: //522/34BF0A000000/SIP/Function/voip_media_dir_to_co_media_dir:


*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/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:


For Video
# Additional References for Network-Based Recording

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MediaSense Installation and Administration Guide</td>
<td>Cisco MediaSense Installation and Administration Guide</td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3984</td>
<td>RTP Payload Format for H.264 Video</td>
</tr>
<tr>
<td>RFC 5104</td>
<td>Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)</td>
</tr>
<tr>
<td>RFC 5168</td>
<td>XML Schema for Media Control</td>
</tr>
</tbody>
</table>
CHAPTER 13

Video Recording - Additional Configurations

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 for Video Recording - Additional Configurations, page 133
- Information About Additional Configurations for Video Recording, page 134
- How to Configure Additional Configurations for Video Recording, page 135
- Verifying Additional Configurations for Video Recording, page 138

Feature Information for Video Recording - Additional Configurations

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 16: Feature Information for Network-Based Recording of Video Calls Using Cisco Unified Border Element

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-Based Recording of Video Calls Using Cisco Unified Border Element</td>
<td>15.3(3)M Cisco IOS XE Release 3.10S</td>
<td>The Network-Based Recording of Video Calls Using Cisco Unified Border Element feature supports software-based forking and recording of video calls. 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.</td>
</tr>
</tbody>
</table>

Information About Additional Configurations for Video Recording

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).
How to Configure Additional Configurations for Video Recording

Enabling FIR for Video Calls (Using RTCP of 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example: Device(config)# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>media profile video media-profile-tag</td>
</tr>
<tr>
<td>Example: Device(config)# media profile video 1</td>
<td>Configures a video media profile and enters media profile configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td>Example: Device(config)# media profile video 1</td>
<td>Enables FIR using the RTCP or SIP INFO method.</td>
</tr>
<tr>
<td>• ref-frame-req rtcp retransmit-count retransmit-number</td>
<td></td>
</tr>
<tr>
<td>• ref-frame-req sip-info</td>
<td></td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
   enable           | Enables privileged EXEC mode. |
| **Example:**     |         |
| Device> enable    |         |
| **Step 2**
   configure terminal | Enters global configuration mode. |
| **Example:**     |         |
| Device# configure terminal |         |
| **Step 3**
   media profile video media-profile-tag | Configures a video media profile and enters media profile configuration mode. |
| **Example:**     |         |
| Device(config)# media profile video 1 |         |
### 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 IDR.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. media profile video media-profile-tag
4. monitor-ref-frames
5. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 media profile video media-profile-tag</td>
<td>Configures a video media profile and enters media profile configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# media profile video 1</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Additional Configurations for Video Recording

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
   
   Enables privileged EXEC mode.
   
   **Example:**
   
   Device> enable

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

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 990057 | include VideoSipInfoIntraFrameRequestCount

   Main call legs
   VideoSipInfoIntraFrameRequestCount=0
   VideoSipInfoIntraFrameRequestCount=0

   CUBE does not generate FIR request on forked leg
   VideoSipInfoIntraFrameRequestCount=0
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.
Verifying Additional Configurations for Video Recording
TDoS Attack Mitigation

The TDoS Attack Mitigation feature enables Cisco Unified Border Element (Cisco UBE) to not respond to Session Initiation Protocol (SIP) requests from IP addresses that are not listed in a trusted IP address list. Cisco UBE validates only out-of-dialog SIP requests against IP addresses in the trusted IP address list. It does not validate in-dialog SIP requests because such requests usually arrive from trusted entities. The TDoS Attack Mitigation feature is supported both on IPv4 and IPv6 networks.

- Finding Feature Information, page 141
- Information About TDoS Attack Mitigation, page 141
- How to Configure TDoS Attack Mitigation, page 142
- Verifying TDoS Attack Mitigation, page 145
- Configuration Examples for TDoS Attack Mitigation, page 146
- Feature Information for TDoS Attack Mitigation, page 147

Finding Feature Information

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

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

Information About TDoS Attack Mitigation

The TDoS Attack Mitigation feature prevents Cisco Unified Border Element (Cisco UBE) from responding to Session Initiation Protocol (SIP) requests arriving from untrusted IP addresses, which leads to an improvement in performance. The SIP stack authenticates the source IP address of an incoming SIP request and blocks the response if the source IP address does not match any IP address in the trusted IP address list. To create a trusted IP address list, you may configure a list of IP addresses or use the IP addresses that have been configured using the session target command in dial-peer configuration mode.
Cisco UBE does not respond to REGISTER requests and consumes REGISTER requests if you configure it only for Telephony Denial-of-Service (TDoS) Attack Mitigation and not as a registrar server.

If you configure Cisco UBE as a registrar server for TDoS attack mitigation, it consumes responses for REGISTER requests that do not belong to any application. Cisco UBE does not consume responses to REGISTER requests that belong to a registrar application.

Note

A SIP registrar is a server that accepts REGISTER requests and is typically collocated with a proxy or redirect server.

Syslogs are printed on the device console every 60 minutes after Cisco UBE consumes a threshold value of 1000 SIP requests.

How to Configure TDoS Attack Mitigation

Configuring 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example</strong>: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example</strong>: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters global VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example</strong>: Device(config)# voice service voip</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address trusted list</td>
<td>Enters IP address trusted list mode and enables the addition of valid IP addresses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(conf-voi-serv)# ip address trusted list</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 ipv4-address [network-mask]</td>
<td>Allows you to add up to 100 IPv4 addresses in the IP address trusted list. Duplicate IP addresses are not allowed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(cfg-iptrust-list)# ipv4 192.0.2.1</td>
<td></td>
</tr>
</tbody>
</table>

- The *network-mask* argument allows you to define a subnet IP address.

**Step 6**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 ipv6-address</td>
<td>Allows you to add IPv6 addresses to the trusted IP address list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(cfg-iptrust-list)# ipv6 2001:DB8:0:ABCD::1/48</td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(cfg-iptrust-list)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring TDoS Attack Mitigation

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. ip address trusted authenticate
5. allow-connections from-type to to-type
6. sip
7. no registrar server
8. silent-discard untrusted
9. end
10. show sip-ua statistics
11. clear sip-ua statistics
### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>voice service voip</td>
<td>Enters voice service configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address trusted authenticate</td>
<td>Enables IP address authentication on incoming H.323 or Session Initiation Protocol (SIP) trunk calls for toll fraud prevention support.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(conf-voi-serv)# ip address trusted authenticate</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>allow-connections <em>from-type to to-type</em></td>
<td>Allows connections between specific types of endpoints in a Cisco UBE.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(conf-voi-serv)# allow-connections sip to sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>no registrar server</td>
<td>Disables the local SIP registrar.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(conf-serv-sip)# no registrar server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>silent-discard untrusted</td>
<td>Discards SIP requests from untrusted sources on an incoming SIP trunk.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(conf-serv-sip)# silent-discard untrusted</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(conf-serv-sip)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>show sip-ua statistics</td>
<td>(Optional) Displays response, traffic, and retry SIP statistics.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show sip-ua statistics</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
------------------|-------------------------------------------------
Step 11 clear sip-ua statistics  | (Optional) Resets the SIP user agent (UA) statistical counters to zero.

### Verifying TDoS Attack Mitigation

#### Sample output for the show sip-ua statistics command

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

```
Device# 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, OkRegister 0/0
    OkSubscribe 0/0, OkNotify 0/0, OkPublish 0/0
    OkInfo 0/0, OkUpdate 0/0,
    202Accepted 0/0, OkOptions 0/0

  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,
    ConditionalRequestFailed 0/0,
    ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
    UnsupportedMediaType 0/0, UnsupportedURI 0/0,
    BadExtension 0/0, TempNotAvailable 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, RequestPending 0/0,
    UnsupportedResourcePriority 0/0,
    Total untrusted Request Consumed 1500, //This counter increments (+1) on reception of an untrusted SIP request.//
    Untrusted Request Consumed in last lap 300, //This counter is updated after every 60 minutes.//
    Last Threshold for Untrusted Request Consumed 1000 //This counter activates when the router boots up. Counter value is the number of untrusted requests that are consumed (after crossing 1000 SIP requests) in each interval of 60 minutes after the router boots up.//

  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, Update 0/0,
  Subscribe 0/0, Notify 0/0, Publish 0/0
  Refer 0/0, Info 0/0,
  Register 0/0

Retry Statistics
  Invite 0, Bye 0, Cancel 0, Response 0,
  Prack 0, Reliable1xx 0, Notify 0, Info 0
  Register 0 Subscribed 0 Update 0 Options 0
  Publish 0

SDP application statistics:
  Parses: 0, Builds 0
  Invalid token order: 0, Invalid param: 0
  Not SDP desc: 0, No resource: 0

Last time SIP Statistics were cleared: <never>

Configuration Examples for TDoS Attack Mitigation

Example: Trusted IP Address List Configuration

The following example shows how to configure a Trusted IP Address list.

Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(config-voi-serv)# ip address trusted list
Device(config-voi-serv)# ipv4 192.0.2.1
Device(config-voi-serv)# ipv6 2001:DB8:0:ABCD::1/48

Example: TDoS Attack Mitigation Configuration

The following example shows how to configure TDoS Attack Mitigation.

Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(config-voi-serv)# ip address trusted authenticate
Device(config-voi-serv)# allow-connections sip to sip
Device(config-voi-serv)# sip
Device(config-voi-serv)# no registrar server
Device(config-voi-serv)# silent-discard untrusted
Feature Information for TDoS Attack Mitigation

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

Table 17: Feature Information for TDoS Mitigation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDoS Attack Mitigation</td>
<td>15.3(3)M</td>
<td>The TDoS Attack Mitigation feature enables Cisco UBE to not respond to Session Initiation Protocol (SIP) requests from IP addresses that are not listed in a trusted IP address list.</td>
</tr>
<tr>
<td>TDoS Attack Mitigation</td>
<td>Cisco IOS XE Release 3.10S</td>
<td>The TDoS Attack Mitigation feature enables Cisco UBE to not respond to Session Initiation Protocol (SIP) requests from IP addresses that are not listed in a trusted IP address list.</td>
</tr>
</tbody>
</table>
CHAPTER 15

Cisco Unified Communications Gateway Services--Extended Media Forking

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 for Cisco Unified Communications Gateway Services—Extended Media Forking, page 149
- Restrictions for Unified Communications Gateway Services—Extended Media Forking, page 150
- Information About Cisco Unified Communications Gateway Services, page 151
- How to Configure UC Gateway Services, page 157
- Configuration Examples for UC Gateway Services, page 163

Feature Information for Cisco Unified Communications Gateway Services—Extended Media Forking

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 Cisco Unified Communications Gateway Services

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Gateway Services</td>
<td>15.3(3)M Cisco IOS XE Release 3.10S</td>
<td>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 RTP and SRTP calls.</td>
</tr>
<tr>
<td>UC Gateway Services API Support for Secure RTP Forking</td>
<td>15.4(3)M Cisco IOS XE Release 3.13S</td>
<td>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 RTP and SRTP calls.</td>
</tr>
</tbody>
</table>

Restrictions for Unified Communications Gateway Services—Extended Media Forking

- Media renegotiation is not supported.
- Media mixing on forked media streams is not supported.
- recordTone insertion is not supported with SRTP calls.
- mediaForkingReason tag is only to notify midcall stream events; notification for events such as codec change is not supported.
- Only voice media stream is supported.
- Supplementary services are not supported.
Information About Cisco Unified Communications Gateway Services

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 3: 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.
Media Forking for SRTP Calls

- 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.

Crypto Tag

For SRTP forking, the optional Crypto tag in NotifyXmfConnectionData or NotifyXmfCallData message indicates the context of an actively forked SRTP connection.

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 mastery 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

<table>
<thead>
<tr>
<th>Original SIP SDP Crypto Offer</th>
<th>SIP SDP Crypto Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>v=0</td>
<td>v=0</td>
</tr>
<tr>
<td>o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98</td>
<td>o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98</td>
</tr>
<tr>
<td>s=SIP Call</td>
<td>s=SIP Call</td>
</tr>
<tr>
<td>c=IN IP4 172.18.193.98</td>
<td>c=IN IP4 172.18.193.98</td>
</tr>
<tr>
<td>t=0 0</td>
<td>t=0 0</td>
</tr>
<tr>
<td>m=audio 51372 RTP/SAVP 0</td>
<td>m=audio 49170 RTP/SAVP 0</td>
</tr>
<tr>
<td>a=rtpmap:0 PCMU/8000</td>
<td>a=rtpmap:0 PCMU/8000</td>
</tr>
<tr>
<td>a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:0Rmdmc0VCspEc3QGZmNpVLEfffHfF1Aw8Sej</td>
<td>a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:NzB4d1BINUAvLEw6UzF3WSj+Ps fizpXShpX1Zj</td>
</tr>
</tbody>
</table>

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 Cisco UBE. Recording tone is played to the parties involved in the call based on the recordTone parameter set in the media forking request.

*Figure 4: 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
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 5: Forking Preservation](image)

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 Cisco UBE.

- 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.

How to Configure UC Gateway Services

Configuring 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip http server</td>
<td>Enables the HTTP server (web server) on the system.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>ip http max-connections value</code></td>
<td>Sets the maximum number of concurrent connections to the HTTP server that will be allowed. The default value is 5.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip http max-connection 100</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>ip http timeout-policy idle seconds life seconds requests value</code></td>
<td>Sets the characteristics that determine how long a connection to the HTTP server should remain open. The characteristics are:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip http timeout-policy idle 600 life 86400 requests 86400</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>http client connection idle timeout seconds</code></td>
<td>Sets the number of seconds that the client waits in the idle state until it closes the connection.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# http client connection idle timeout 600</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>uc wsapi</code></td>
<td>Enters Cisco Unified Communication IOS Service configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# uc wsapi</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>message-exchange max-failures number</code></td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# message-exchange max-failures 2</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>probing max-failures number</code></td>
<td>Configures the maximum number of failed probing messages before the router unregisters the application. Range is 1 to 5. Default is 3.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# probing max-failures 5</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td><code>probing interval keepalive seconds</code></td>
<td>Configures the maximum number of failed probing messages before the router unregisters the application. Range is 1 to 5. Default is 3.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# probing interval keepalive 255</td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>probing interval negative seconds</code></td>
<td>Configures the interval between negative probing messages, in seconds.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# probing interval negative 10</td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td><code>source-address ip-address</code></td>
<td>Configures the IP address (hostname) as the source IP address for the UC IOS service.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# source-address 192.1.12.14</td>
<td>Note: The source IP address is used by the provider in the NotifyProviderStatus messages.</td>
</tr>
<tr>
<td>Step 13</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the XMF Provider

SUMMARY STEPS

1. enable
2. configure terminal
3. uc wsapi
4. provider xmf
5. no shutdown
6. remote-url index url
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> uc wsapi</td>
<td>Enters Cisco Unified Communication IOS Service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# uc wsapi</td>
</tr>
<tr>
<td><strong>Step 4</strong> provider xmf</td>
<td>Enters XMF provider configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# provider xmf</td>
</tr>
<tr>
<td><strong>Step 5</strong> no shutdown</td>
<td>Activates XMF provider.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-uc-wsapi)# no shutdown</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step 6</th>
<th>remote-url index url</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-uc-wsapi)# remote-url 1 <a href="http://test.com:8090/ucm_xmf">http://test.com:8090/ucm_xmf</a></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-uc-wsapi)# end</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

### Verifying 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

<table>
<thead>
<tr>
<th>registration index: 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>id: 2E7C3034:XMF:myapp:26</td>
</tr>
<tr>
<td>appUrl: <a href="http://pascal-lnx.cisco.com:8094/xmf">http://pascal-lnx.cisco.com:8094/xmf</a></td>
</tr>
<tr>
<td>appName: myapp</td>
</tr>
<tr>
<td>provUrl: <a href="http://9.45.46.16:8090/cisco_xmf">http://9.45.46.16:8090/cisco_xmf</a></td>
</tr>
</tbody>
</table>
Step 3  
**show wsoapi 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 wsoapi registration xmf 1
```

**Provider XMF**

```
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
```

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!
### Troubleshooting Tips

You can use the following `debug` commands to troubleshoot the UC Gateway Services configurations.

- `debug wsapi infrastructure all`
- `debug wsapi xcc all`
- `debug wsapi xmf all`
- `debug wsapi xmf messages`
- `debug wsapi infrastructure detail`
- `debug voip application`
- `debug voip application media forking`

### Configuration Examples for UC Gateway Services

#### 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```
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 16

Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

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 (Cisco UBE) interworks between different dynamic payload type values across the call legs for the same codec. Also, Cisco UBE 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 for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls, page 165
- Restrictions for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls, page 166
- Symmetric and Asymmetric Calls, page 167
- High Availability Checkpointing Support for Asymmetric Payload, page 168
- How to Configure Dynamic Payload Type Passthrough for DTMF and Codec Packets for SIP-to-SIP Calls, page 168
- Configuration Examples for Assymetric Payload Interworking, page 172

Feature Information for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

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 19: Feature Information for Dynamic Payload Interworking for DTMF and Codec Packets Support

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls</td>
<td>15.0(1)XA 15.1(1)T</td>
<td>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. The following commands were introduced or modified: <code>asymmetric payload</code> and <code>voice-class sip asymmetric payload</code>.</td>
</tr>
<tr>
<td>Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls</td>
<td>Cisco IOS Release XE 3.1S</td>
<td>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. The following commands were introduced or modified: <code>asymmetric payload</code> and <code>voice-class sip asymmetric payload</code>.</td>
</tr>
<tr>
<td>High Availability Checkpointing Support for Asymmetric Payload</td>
<td>Cisco IOS Release XE 3.12S</td>
<td>High availability support for asymmetric payload type interworking was added.</td>
</tr>
</tbody>
</table>

### Restrictions for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature is not supported for the following:

- H323-to-H323 and H323-to-SIP calls.
- All transcoded calls.
- 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:

\[
m = \text{audio} <\text{media-port1}> \text{ RTP/AVP XXX} \quad m = \text{video} <\text{media-port2}> \text{ RTP/AVP XXX}
\]

## Symmetric and Asymmetric Calls

Cisco UBE supports dynamic payload type negotiation and interworking for all symmetric and asymmetric payload type combinations. A call leg on Cisco UBE 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 Cisco UBE 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 6: Sample High-Availability Topology

How to Configure Dynamic Payload Type Passthrough for DTMF and Codec Packets for SIP-to-SIP Calls

Configuring 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Purpose Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# voice service voip</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters voice service SIP configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(conf-voi-serv)# sip</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> asymmetric payload</td>
<td>Configures global SIP asymmetric payload support.</td>
<td></td>
</tr>
<tr>
<td>{dtmf</td>
<td>dynamic-codecs</td>
<td>full</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(conf-serv-sip)# asymmetric payload full</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits voice service SIP configuration mode and enters privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(conf-serv-sip)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
  **Example:**  
  `Device> enable`  
  • Enter your password if prompted. |
| **Step 2** | `configure terminal` | Enters global configuration mode.  
  **Example:**  
  `Device# configure terminal` |
| **Step 3** | `dial-peer voice tag voip` | Enters dial peer voice configuration mode.  
  **Example:**  
  `Device(config)# dial-peer voice 77 voip` |
| **Step 4** | `voice-class sip asymmetric payload {dtmf | dynamic-codecs | full | system}` | 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.  
  **Example:**  
  `Device(config-dial-peer)# voice-class sip asymmetric payload full` |
| **Step 5** | `end` | (Optional) Exits dial peer voice configuration mode and enters privileged EXEC mode.  
  **Example:**  
  `Device(config-dial-peer)# end` |
Verifying 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>show call active voice compact</code></td>
<td>(Optional) Displays a compact version of call information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show call active voice compact</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>show call active voice</code></td>
<td>(Optional) Displays call information for voice calls in progress.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show call active voice</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

Use the following commands to debug any errors that you may encounter when you configure 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 Assymetric 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
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
!
Example: Asymmetric Payload Interworking—Interworking Configuration
iLBC Support for SIP and H.323

The internet Low Bitrate Codec (iLBC) is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323.

- Finding Feature Information, page 175
- Prerequisites for iLBC Support for SIP and H.323, page 175
- Restrictions for iLBC Support for SIP and H.323, page 176
- Information About iLBC Support for SIP and H.323, page 176
- How to Configure an iLBC Codec, page 176
- Feature Information for iLBC Support for SIP and H.323, page 180

Finding Feature Information

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

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

Prerequisites for iLBC Support for SIP and H.323

Cisco Unified Border Element

- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.
Cisco Unified Border Element (Enterprise)

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

Restrictions for iLBC Support for SIP and H.323

The iLBC Support for SIP and H.323 feature is supported on the following:

- IP-to-IP gateways with no transcoding and conferencing
- All c5510 DSP-based platforms

Information About iLBC Support for SIP and H.323

The internet Low Bit Rate Codec (iLBC) is designed for narrow band speech and results in a payload bit rate of 13.33 kbits per second for 30-millisecond (ms) frames and 15.20 kbits per second for 20 ms frames.

When the codec operates at block lengths of 20 ms, it produces 304 bits per block, which is packetized as defined in RFC 3952. Similarly, for block lengths of 30 ms it produces 400 bits per block, which is packetized as defined in RFC 3952.

The iLBC has built-in error correction functionality to provide better performance in networks with higher packet loss.

How to Configure an iLBC Codec

Configuring an iLBC Codec on a Dial Peer

The iLBC is intended for packet-based communication. Perform the following steps to configure the iLBC codec on a dial peer.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. rtp payload-type cisco-codec-ilbc [number
5. codec ilbc [mode frame_size [bytes payload_size]]
6. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice <em>tag</em> voip</td>
<td>Enters dial-peer configuration mode for the VoIP dial peer designated by <em>tag</em>.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# dial-peer voice 10 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> rtp payload-type cisco-codec-ilbc [number]</td>
<td>Identifies the payload type of a Real-Time Transport Protocol (RTP) packet. Keyword and argument are as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-dial-peer)# rtp payload-type cisco-codec-ilbc 100</td>
<td>• <strong>cisco-codec-ilbc</strong> [number]--Payload type is for internet Low Bit Rate Codec (iLBC). Range: 96 to 127. Default: 116.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not use the following numbers because they have preassigned values: 96, 97, 100, 117, 121 to 123, and 125 to 127. If you use these values, the command will fail. You must first reassign the value in use to a different unassigned number, for example:</td>
</tr>
<tr>
<td></td>
<td>rtp payload-type nse 105</td>
</tr>
<tr>
<td></td>
<td>rtp payload-type cisco-codec-ilbc 100</td>
</tr>
<tr>
<td><strong>Step 5</strong> codec ilbc [mode frame_size [bytes payload_size]]</td>
<td>Specifies the voice coder rate of speech for a dial peer. Keywords and arguments are as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-dial-peer)# codec ilbc mode 30 bytes 200</td>
<td>• <strong>mode</strong> frame_size --The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bytes</strong> payload_size --Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50(default), 100, 150, and 200.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring an iLBC Codec in the Voice Class

When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to VoIP dial peers. The **voice class codec** global configuration command allows you to define the voice class that contains the codec selection order. Then, use the **voice-class codec** dial-peer configuration command to apply the class to individual dial peers.

To configure an iLBC in the voice class for multiple-codec selection order, perform the following steps.

You can configure more than one voice class codec list for your network. Configure the codec lists and apply them to one or more dial peers based on which codecs (and the order) you want supported for the dial peers. Define a selection order if you want more than one codec supported for a given dial peer.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice class codec tag`
4. `codec preference value ilbc [mode frame_size] [bytes payload_size]`
5. `exit`
6. `dial-peer voice tag voip`
7. `voice-class codec tag`
8. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. The argument is as follows:</td>
</tr>
<tr>
<td><code>voice class codec tag</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# voice class codec 99</td>
</tr>
<tr>
<td></td>
<td>• <em>tag</em> --Unique identifier on the router. Range is 1 to 10000.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>codec preference value ilbc [mode frame_size] [bytes payload_size]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-voice-class)# codec preference 1 ilbc 30 200</td>
</tr>
</tbody>
</table>

**Purpose:** Specifies a list of preferred codecs to use on a dial peer. Keywords and arguments are as follows:

- **value** -- Order of preference, with 1 being the most preferred and 14 being the least preferred.
- **mode frame_size** -- The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20.
- **bytes payload_size** -- Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50 (default), 100, 150, and 200.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-voice-class)# exit</td>
</tr>
</tbody>
</table>

**Purpose:** Exits the current mode.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>dial-peer voice tag voip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# dial-peer voice 16 voip</td>
</tr>
</tbody>
</table>

**Purpose:** Enters dial-peer configuration mode for the specified VoIP dial peer.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>voice-class codec tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# voice-class codec 99</td>
</tr>
</tbody>
</table>

**Purpose:** Assigns a previously configured codec selection preference list (the codec voice class that you defined in step 3) to the specified VoIP dial peer.

**Note:** The voice-class codec command in dial-peer configuration mode contains a hyphen. The voice class command in global configuration mode does not contain a hyphen.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config-dial-peer)# exit</td>
</tr>
</tbody>
</table>

**Purpose:** Exits the current mode.

---

### Verifying iLBC Support for SIP and H.323

You can use the following commands to check iLBC status:

- show voice call summary
- show voice call status
• show voice dsmp stream
• show call active voice
• show call history voice
• show voice dsp and its extensions
• show dial-peer voice
• show voice dsp channel operational-status

Feature Information for iLBC Support for SIP and H.323

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 images. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 20: Feature Information for iLBC Support for SIP and H.323

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>iLBC Support for SIP and H.323</td>
<td>12.2(11)T 12.2(15)T</td>
<td>The iLBC is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323. The following commands were introduced or modified: <code>codec ilbc</code>, <code>codec preference</code>, and <code>rtp payload-type</code>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>iLBC Support for SIP and H.323</td>
<td>Cisco IOS XE Release 2.5</td>
<td>The iLBC is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323. The following commands were introduced or modified: <code>codec ilbc</code>, <code>codec preference</code>, and <code>rtp payload-type</code>.</td>
</tr>
</tbody>
</table>
DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating

The DSP-Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating of dspfarm feature provides transcoding support for DSPs that are located on the same box as the Cisco ASR.

- Finding Feature Information, page 183
- Prerequisites for DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating, page 184
- Restrictions for DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating, page 184
- Information About DSP-Based Functionality on Cisco UBE Enterprise Including Transcoding and Transrating, page 184
- How to Configure DSP-Based Functionality on Cisco UBE Enterprise Including Transcoding and Transrating, page 185
- Feature Information for DSP-based functionality on Cisco UBE Enterprise including Transcoding and Transrating, page 187

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating

• To enable this feature, you must have Cisco IOS XE Release 3.2S or a later release installed and running on your Cisco ASR 1000 Series Router.

Restrictions for DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating

• Out-of-box transcoding is not supported.
• Cisco Unified Communications Manager transcoding is not supported.
• Transcoding calls are not check-pointed, when failover happens, these calls will not be persevered. The expected behavior is for the SPA card to reset the DSPs and start the firmware download.

Information About DSP-Based Functionality on Cisco UBE Enterprise Including Transcoding and Transrating

To configure transcoding on the Cisco UBE it was required that architecture a Cisco Unified Communications Manager was required to setup the transcoding streams through SCCP protocol for both inbox and out-of-box transcoding. The result is a significant amount of overhead for the inbox transcoding case with SCCP messaging and additional 2 RTPSPI and VOIP RTP ports associated with the SCCP transcoding call leg. The DSP-based functionality feature avoids addition resource overhead for inbox transcoding by having DSMP streams setup via VOIP FPI by the SPI legs bypassing the requirement for SCCP client, SCCP server and RTPSPI streams for inbox transcoding. The transcoding conversion in the Cisco UBE (Enterprise) is completed in the Ucode library. The DSP farm profile guarantees the configured resources for the most complex codec that is configured.

DTMF interoperability for transcoding calls is supported for the following call flows:
• RFC2833 <--> OOB
• RFC2833 <--> RFC2833
• Inband Tone <--> RFC2833

Note
Inband <--> OOB is not supported currently by the CUBE (Enterprise).
How to Configure DSP-Based Functionality on Cisco UBE Enterprise Including Transcoding and Transrating

To configure DSP-Based Functionality on the Cisco UBE (Enterprise) including Transcoding and Transrating perform the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dspfarm profile
   - Cisco Unified Border Element
   - Cisco Unified Border Element (Enterprise)
4. codec {codec-type | pass-through}
5. maximum sessions number
6. associate application {cube | sbc | sccp}
7. no shutdown
8. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>dspfarm profile</td>
<td>Enters the DSP farm profile configuration mode and defines a profile for digital signal processor (DSP) farm services.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>SRTP support on the Cisco Unified Border Element is provided via a transcoding profile. SRTP support on the Cisco Unified Border Element (Enterprise) is provided through library.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>dspfarm profileprofile-identifier transcode</strong></td>
<td></td>
</tr>
<tr>
<td>Device# dspfarm profile 2 transcode</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

**codec** \{\textit{codec-type} | pass-through\}

**Example:**
Device (config-dspfarm-profile)# codec g711ulaw

Specifies the codecs supported by a DSP farm profile. Repeat this step for each codec supported by the profile.

**Note**
- Hardware MCPO support only G.711 a-law and G.711 u-law. If you configure a profile as a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the no maximum sessions hardware command.
- Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

**Step 5**

**maximum sessions** \textit{number}

**Example:**
Device (config-dspfarm-profile)# maximum sessions 768

Specifies the maximum number of sessions that are supported by the profile.

- **number** -- Range is determined by the available registered DSP resources. Default is 0.

**Note**
The hardware and software keywords apply only to MTP profiles.

**Step 6**

**associate application** \{cube | sbc | sccp\}

**Example:**
Device (config-dspfarm-profile)# associate application cube

Associates the application to the DSP profile.

**Step 7**

**no shutdown**

**Example:**
Device (config-dspfarm-profile)# no shutdown

Enables the profile, allocates DSP farm resources, and associates the application.

**Step 8**

**exit**

**Example:**
Device (config-dspfarm-profile)# exit

Exits DSP farm profile configuration mode.

**Verifying DSP Farm Configuration**

To verify DSP-based functionality on Cisco UBE (Enterprise) including Transcoding and Transrating of dspfarm feature use the following commands:
• **show voice dsp group** — Displays the DSP resource allocation, the total number of credits, and number of credits and channels in use.

• **show dspfarm dsp** — Display the dsp allocated to the dspfarm.

• **show dspfarm dsp stats** — Displays statistics for each dsp session.

---

**Feature Information for DSP-based functionality on Cisco UBE Enterprise including Transcoding and Transrating**

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 21: Feature Information for DSP-based functionality on Cisco UBE including Transcoding and Transrating**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSP Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating</td>
<td>Cisco IOS XE Release 3.2S</td>
<td>Provides transcoding support for DSPs that are located on the same box as the Cisco UBE (Enterprise). The following commands were modified: <strong>associate application, codec, and dspfarm profile.</strong></td>
</tr>
</tbody>
</table>
Acoustic Shock Protection

Acoustic Shock Protection (ASP) is a voice circuit-breaker feature that is designed to protect users, especially those wearing headsets, from exposure to loud, sustained, and piercing tones, such as those produced by a fax machine. It is a workplace-safety feature for voice calls. When the tone is present at the input of the ASP module, the audio path in the affected direction is muted to protect the listener, and a gentle alert tone is played out for as long as the tone persists. ASP may be inserted in either or both directions of a call, that is, applied to incoming packets to protect the ears of a listener on the Time-Division Multiplexing (TDM) gateway, applied to incoming PSTN calls (microphone signal) to protect the ears of listeners at the other end of the call, or applied to both simultaneously.

- Finding Feature Information, page 189
- Restrictions for ASP, page 189
- Information About ASP, page 190
- How to Configure ASP, page 191
- Configuration Examples for the Acoustic Shock Protection Feature, page 196
- Feature Information for Acoustic Shock Protection, page 197

Finding Feature Information

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

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

Restrictions for ASP

- Supported on PVDM3 only.
- Supported only on flex codec complexity.
• No support for H.32x video call, complex forking calls, and fax and modem calls.
• No support for TDM hairpin call.
• The configuration under dial peer has higher priority than the configuration at the global level.
• No support for conference calls, IP/SIP phones, and the Skinny Client Control Protocol (SCCP).
• CLI supports enabling ASP but not disabling ASP.
• No support for dynamically enabling or disabling ASP during a call.

Information About ASP

Acoustic Shock Protection

Acoustic Shock Protection (ASP) is an adaptive signal processing algorithm on the Digital Signal Processor (DSP) that analyzes incoming audio for the presence of offending tones that might harm humans. Offending tones include signals that are:

• Loud
• Tonal (energy concentrated around a single frequency)
• Persistent (lasts longer than a few tens of milliseconds)

If an offending tone is present, the audio path in that direction is muted temporarily, and a quiet, alerting signal is played out to the listener side. The call is never dropped; only the audio is muted temporarily. If or when the tone disappears from the input, the mute is removed. ASP does not disrupt low-frequency tones (below 650 Hz) such as ringback, dial, and so forth. Since ASP is designed to mute only single-frequency tones, it allows multi-tone signals such as Dual Tone Multi-Frequency (DTMF) to pass unhindered. ASP is supported on TDM gateways (TDM-VoIP and TDM-TDM) and on the Cisco Unified Border Element (Cisco UBE).

ASP is for voice calls only and not for faxes and modems.

Some of the best practices for ASP are as follows:

• Use default values
• Use ASP on dial peers where you are certain that people (not faxes) are listening.
• Do not use ASP on dial peers associated with fax machines, modems, or TTY/TDD devices. Use fax-relay or modem-relay modes on dial peers dedicated to such devices.
• ASP is designed for deployment in situations where customers have experienced acoustic shock safety issues. If there are issues like false triggering (for example, ASP alerts on regular voices), then you must turn off ASP. You can choose from three detector sensitivity modes: slow, auto, or fast. Fast mode is a highly sensitive hair-trigger. Auto mode is recommended. Slow mode lets more tone leak through, but has better rejection of false triggers.
How to Configure ASP

Creating the Media Profile for ASP

Perform this task to create a media profile to configure acoustic shock protection.

SUMMARY STEPS

1. enable
2. configure terminal
3. media profile asp *tag*
4. mode *mode*
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>media profile asp <em>tag</em></strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# media profile asp 5</td>
</tr>
<tr>
<td></td>
<td>Creates the media profile to configure ASP and enters media profile</td>
</tr>
<tr>
<td></td>
<td>configuration mode. The range for the media profile tag is from 1 to</td>
</tr>
<tr>
<td></td>
<td>10000.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>mode <em>mode</em></strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(cfg-mediaprofile)# mode auto</td>
</tr>
<tr>
<td></td>
<td>Sets the ASP sensitivity mode to preset = auto (which is default). Auto</td>
</tr>
<tr>
<td></td>
<td>mode provides a good tradeoff between ASP speed and false trigger</td>
</tr>
<tr>
<td></td>
<td>rejection.</td>
</tr>
<tr>
<td></td>
<td>The other modes are:</td>
</tr>
<tr>
<td></td>
<td>• slow—Presets ASP sensitivity mode to 1. This mode provides slower</td>
</tr>
<tr>
<td></td>
<td>detection speed for reduced chance of false triggers.</td>
</tr>
<tr>
<td></td>
<td>• fast—Presets ASP sensitivity mode to 2. This mode provides faster</td>
</tr>
<tr>
<td></td>
<td>detection speed but higher chance of false triggers.</td>
</tr>
<tr>
<td></td>
<td>• expert—This mode exposes direct control of individual ASP parameters</td>
</tr>
<tr>
<td></td>
<td>and is recommended for test use only.</td>
</tr>
</tbody>
</table>
### Creating the Media Profile to Enable ASP

After the media profile is created, you must create a media class to enable acoustic shock protection. Perform this task to create a media class.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `media class tag`
4. `asp profile tag`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device#</code> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>media class tag</code></td>
<td>Creates the media class to enable the acoustic shock protection feature and enters media class configuration mode. The range for the media class tag is from 1 to 10000.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# media class 2</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Media Class at a Dial Peer Level for ASP

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag pots`
4. `media-class tag`
5. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>dial-peer voice tag pots</code></td>
<td>Defines a particular dial peer and enters dial-peer voice configuration mode. The range for the dial-peer voice tag is from 1 to 1073741823.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# dial-peer voice 20 pots</code></td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

- `asp profile tag`  
  Applies the media profile to the media class. The range for the media profile ASP tag is from 1 to 10000.

- `end`  
  Returns to privileged EXEC mode.
### Purpose

**Command or Action**

**Step 4**

`media-class tag`

**Example:**

Device(config-dial-peer)# media-class 2

Applies the media class to the specific dial peer. The range for the media class tag number is from 1 to 10000.

**Step 5**

`end`

**Example:**

Device(config-dial-peer)# end

Returns to privileged EXEC mode.

---

### Configuring the Media Class Globally for ASP

**SUMMARY STEPS**

1. enable
2. configure terminal
3. media service
4. enhancement
5. tdm `tag`
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>media service</code></td>
<td>Enters media service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# media service</td>
<td></td>
</tr>
</tbody>
</table>
### Verifying ASP

Perform this task to verify the voice quality metrics.

**SUMMARY STEPS**

1. **enable**
2. **show call active voice stats | b pid:**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; <strong>enable</strong></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>**show call active voice stats</td>
<td>b pid:**</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# **show call active voice stats</td>
<td>b pid:1300**</td>
</tr>
</tbody>
</table>

```
11EC : 5 09:14:25.971 PDT Thu Jul 28 2011.1 +1130 pid:1300 Answer 1300 active dur 00:01:36 tx:17/321 rx:17/321 dscp:0 media:0
DSP/TX: PK=17, SG=0, NS=1, DU-90570, VO=320
DSP/RX: PK=17, SG=0, CP=1, RX-90570, VO=320, BS=0, BP=0, LP=0, EP=0
```
Troubleshooting Tips

The following commands can help troubleshoot ASP:

- debug voip hpi all
- debug voip dsmpp all
- debug voip dsm all
- debug voip vsmp all
- debug vpm dsp all

Configuration Examples for the Acoustic Shock Protection Feature

**Example: Enabling ASP Globally**

```xml
media profile asp 6
!
media class 1
  asp profile 6
!
media service
  enhancement
tdm 1
```

**Example: Enabling ASP on a Dial Peer**

```xml
media profile asp 4
!
media class 1
  asp profile 4
!
dial-peer voice 2100 pots
  destination-pattern 2100
  incoming called-number 1100
```
Feature Information for Acoustic Shock Protection

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 22: Feature Information for Acoustic Shock Protection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acoustic Shock Protection</td>
<td>15.2(2)T, 15.2(3)T</td>
<td>Acoustic Shock Protection (ASP) is a voice circuit-breaker feature that is designed to protect users, especially those wearing headsets, from exposure to loud, sustained, and piercing tones, such as those produced by a fax machine. It is a workplace-safety feature for voice calls. ASP is supported on TDM gateways and on Cisco UBE. The following commands were introduced or modified: media profile asp, media service.</td>
</tr>
<tr>
<td>Acoustic Shock Protection</td>
<td>Cisco IOS XE Release 3.6S</td>
<td>Acoustic Shock Protection (ASP) is a voice circuit-breaker feature that is designed to protect users, especially those wearing headsets, from exposure to loud, sustained, and piercing tones, such as those produced by a fax machine. It is a workplace-safety feature for voice calls. ASP is supported on TDM gateways and on Cisco UBE. In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise) The following commands were introduced or modified: media profile asp, media service.</td>
</tr>
</tbody>
</table>
Noise Reduction

Noise Reduction (NR) is a voice enhancement process that improves the quality of incoming speech that has already been corrupted with background noise; for example, a voice conference participant speaking on a cell-phone in a car. NR works best with steady state broadband noises like engine noise but not as well with impulsive noises like nearby chatter.

- Finding Feature Information, page 199
- Prerequisites for Noise Reduction, page 199
- Restrictions for NR, page 200
- Information About NR, page 200
- How to Configure NR, page 201
- Configuration Examples for the NR feature, page 206
- Feature Information for Noise Reduction, page 207

Finding Feature Information

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

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

Prerequisites for Noise Reduction

Cisco Unified Border Element

- Cisco IOS Release 15.2(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 3.6 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for NR

- Supported only on PVDM3.
- Supported only on flex codec complexity.
- No support for H.32x video call, complex forking calls, and fax and modem calls.
- No support for Time-Division Multiplexing (TDM) hairpin call.
- Configurations under POTS dial peer has higher priority over VoIP dial peer for NR.
- Configurations under the dial peer has higher priority than configurations at the global level.
- No support for conference calls, IP/SIP phones, and the Skinny Client Control Protocol (SCCP).
- CLI supports enabling NR but not disabling NR.
- No support for dynamically enabling or disabling NR during a call.

Information About NR

Noise Reduction

Noise Reduction (NR) is an adaptive signal processing algorithm on the Digital Signal Processor (DSP) that analyzes incoming audio, extracts a fingerprint of the background noise during talker pauses, and then performs ongoing spectral subtraction of this noise after a short training period (a few seconds). NR constantly adapts to changes in background noises over time.

NR can affect music on hold signals by making the music quieter. NR may disrupt fax/modem/TDD devices, although it is designed to self-disable in those cases. Use modem-relay mode for reliable fax/modem transmission. NR is supported on TDM gateways (TDM-VoIP and TDM-TDM) and on the Cisco Unified Border Element (Cisco UBE).

Some of the best practices for NR are as follows:

- Use default values.
- Do not use NR on dial peers associated with fax machines. Use fax or modem-relay modes for those dial peers.
- NR, when used without dynamic user control of intensity (as is the case with gateways), must be used at a low intensity (default or lower) since it is always on. High intensity is dramatic for demonstrations with loud background noises, but the NR process itself will degrade "normal" calls if NR is run at high intensity.
How to Configure NR

Creating the Media Profile for NR

Perform this task to create a media profile to configure noise reduction parameters.

SUMMARY STEPS

1. enable
2. configure terminal
3. media profile nr tag
4. intensity level
5. noisefloor level
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> media profile nr tag</td>
<td>Creates the media profile to configure noise reduction parameters and enters media profile configuration mode. The range for the media profile tag is from 1 to 10000.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# media profile nr 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> intensity level</td>
<td>Configures the intensity level or depth of the noise reduction process. The range is from 0 to 6.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(cfg-mediaprofile)# intensity 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> noisefloor level</td>
<td>Configures the noise level, in dBm, above which NR will operate. NR will allow noises quieter than this level to pass without processing. The range is from -58 to -20.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(cfg-mediaprofile)# noisefloor -50</td>
<td></td>
</tr>
</tbody>
</table>
Creating the Media Class to Enable NR

After the media profile is created, you must create a media class to enable noise reduction. Perform this task to create a media class.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. media class tag
4. nr profile tag
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td>enable</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Example:</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td>media class tag</td>
<td>nr profile tag</td>
</tr>
<tr>
<td>Example:</td>
<td>Example:</td>
</tr>
<tr>
<td>Device(config)# media class 2</td>
<td>Device(config)# nr profile 2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Noise Reduction

### Configuring the Media Class at a Dial Peer Level for NR

Perform this task to configure the media class for a dial peer.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag pots`
4. `media-class tag`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice</td>
<td>Defines a particular dial peer and enters the dial-peer voice</td>
</tr>
<tr>
<td><code>tag pots</code></td>
<td>configuration mode. The range for the dial-peer voice tag is</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# dial-peer voice 20 pots</code></td>
<td>from 1 to 1073741823.</td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
---|---
Step 4 | media-class \textit{tag}  
Example: Device\{config-dial-peer\}# media-class 2  
Applies the media class to the specific dial peer. The range for the media class tag number is from 1 to 10000.

Step 5 | end  
Example: Device\{config-dial-peer\}# end  
Returns to the privileged EXEC mode.

---

### Configuring the Media Class Globally for NR

Perform this task to configure a media class globally.

#### SUMMARY STEPS

1. enable  
2. configure terminal  
3. media service  
4. enhancement  
5. tdm \textit{tag}  
6. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> media service</td>
<td>Enters media service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# media service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enhancement</td>
<td>Enters the submode enhance of media service.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(cfg-mediaservice)# enhancement</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> tdm tag</td>
<td>Applies the TDM call globally. The range for the media class tag number is from 1 to 10000.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(cfg-service-enhance)# tdm 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying NR

Perform this task to verify the voice quality metrics.

#### SUMMARY STEPS

1. enable  
2. show call active voice stats | b pid:

#### DETAILED STEPS

**Step 1** enable

**Example:**  
Device> enable

Enables privileged EXEC mode.

**Step 2** show call active voice stats | b pid:
Example:
Device# show call active voice stats | b pid:1300

11EC : 5 09:14:25.971 PDT Thu Jul 28 2011.1 +1130 pid:1300 Answer 1300 active dur 00:01:36 tx:17/321 rx:17/321 dscp:0 media:0
DSP/TX: PK=17, SG=0, NS=1, DU=90570, VO=320
DSP/RX: PK=17, SG=0, CF=1, RX=90570, VO=320, BS=0, BP=0, LP=0, EP=0

... DSP/DL: RT=0, ED=0
MIC Direction:
DSP/NR: NR=1, ND=0, LV=257, IN=1, PN=0, ON=0
DSP/AS: AE=1, AD=0, AV=0, AM=0, NT=0, DT=0, TT=0, TD=0, LP=0, LD=0
EAR Direction:
DSP/NR: NR=0, ND=0, LV=0, IN=0, PN=0, ON=0
DSP/AS: AE=0, AD=0, AV=0, AM=0, NT=0, DT=0, TT=0, TD=0, LP=0, LD=0


Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1

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

Troubleshooting Tips

The following commands can help troubleshoot NR:

- debug voip hpi all
- debug voip dsmp all
- debug voip dsm all
- debug voip vtsp all
- debug vpm dsp all

Configuration Examples for the NR feature

Example: Enabling NR globally

```
media profile nr 1
  intensity 1
!
media profile nr 2
!
media profile nr 3
  intensity 2
!
media profile nr 4
  intensity 3
!
media profile nr 5
  intensity 2
```
Feature Information for Noise Reduction

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 23: Feature Information for Noise Reduction

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noise Reduction</td>
<td>15.2(2)T, 15.2(3)T</td>
<td>Noise Reduction (NR) is a voice enhancement or restoration process that improves the quality of incoming speech that has already been corrupted with background noise. NR is supported on TDM gateways and on the Cisco UBE. The following commands were introduced or modified: intensity, media profile nr, media service, and noisefloor.</td>
</tr>
<tr>
<td>Noise Reduction</td>
<td>Cisco IOS XE Release 3.6S</td>
<td>Noise Reduction (NR) is a voice enhancement or restoration process that improves the quality of incoming speech that has already been corrupted with background noise. NR is supported on TDM gateways and on Cisco UBE. In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: intensity, media profile nr, media service, noisefloor.</td>
</tr>
</tbody>
</table>
CHAPTER 21

SIP Ability to Send a SIP Registration Message on a Border Element

• Finding Feature Information, page 209
• Prerequisites for SIP Ability to Send a SIP Registration Message on a Border Element, page 209
• Configuring SIP Ability to Send a SIP Registration Message on a Border Element, page 210
• Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element, page 211

Finding Feature Information

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

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

Prerequisites for SIP Ability to Send a SIP Registration Message on a Border Element

• Configure a registrar in sip UA configuration mode.

Cisco Unified Border Element

• Cisco IOS Release 12.4(24)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
• Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

## Configuring SIP Ability to Send a SIP Registration Message on a Border Element

The SIP: Ability to Send a SIP Registration Message on a Border Element feature allows users to register E.164 numbers from the Cisco UBE without POTS dial-peers in the UP state. Registration messages can include numbers, number ranges (such as E.164-numbers), or text information.

### SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. credentials username *username* password *password* realm *domain-name*
5. exit
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters sip user-agent configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> credentials username <em>username</em> password <em>password</em> realm <em>domain-name</em></td>
<td>Enters SIP digest credentials in sip-ua configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-sip-ua)# credentials username alex password test realm cisco.com</td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
**Step 5** |  
exit | Exits the current mode.

**Example:**

Device(config-sip-ua)# exit

**Step 6** |  
end | Returns to privileged EXEC mode.

**Example:**

Device(config)# end

---

**Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element**

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP: Ability to Send a SIP Registration Message on a Border Element</td>
<td>12.4(24)T</td>
<td>Provides the ability to send a SIP Registration Message from Cisco Unified Border Element. The following command was modified: <strong>credentials</strong> (SIP UA)</td>
</tr>
<tr>
<td>SIP: Ability to Send a SIP Registration Message on a Border Element</td>
<td>Cisco IOS XE Release 2.5</td>
<td>Provides the ability to send a SIP Registration Message from Cisco Unified Border Element. The following command was modified: <strong>credentials</strong> (SIP UA)</td>
</tr>
</tbody>
</table>
SIP Profiles

Session Initiation Protocol (SIP) profiles change SIP incoming or outgoing messages so that interoperability between incompatible devices can be ensured.

SIP profiles can be configured 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 7: Incoming and Outgoing messages where SIP Profiles can be applied

You can use the following tool to test your SIP profile on an incoming message.
http://cantor.cisco.com/sip-profiles.html

- Feature Information for SIP Profiles, page 213
- Information About SIP Profiles, page 215
- Restrictions for SIP Profiles, page 217
- How to Configure SIP Profiles, page 218

Feature Information for SIP Profiles

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 SIP Profiles

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Profiles (for inbound messages)</td>
<td>Cisco IOS 15.4(2)T Cisco IOS XE 3.12S</td>
<td>This feature extends support to inbound messages. This feature modifies the following commands: The <strong>inbound</strong> keyword was added to the <strong>sip-profiles</strong> and <strong>voice-class sip profiles</strong> commands.</td>
</tr>
<tr>
<td>Support for Rotary calls and Media Forking</td>
<td>Cisco IOS 15.3(1)T</td>
<td>With CSCty41575, this feature was enhanced to support forked and rotary calls.</td>
</tr>
<tr>
<td>Configuring SIP Profile (Add, Delete or Modify)</td>
<td>Cisco IOS 12.4(15)XZ Cisco IOS 12.4(20)T Cisco IOS XE 2.5</td>
<td>This feature allows users to change (add, delete, or modify) the standard SIP messages that are sent or received for better interworking with different SIP entities. This feature introduces the following commands: <strong>voice class sip-profiles</strong>, <strong>response</strong>, <strong>request</strong>.</td>
</tr>
<tr>
<td>Support for Non-Standard SIP Headers</td>
<td>Cisco IOS 15.5(2)T</td>
<td>This feature allows users to add, copy, delete, or modify non-standard (for example, X-Cisco-Recording-Participant) using SIP profiles. The <strong>word</strong> keyword was added to the <strong>sip-profiles</strong> command to allow the user to configure any non-standard SIP header.</td>
</tr>
</tbody>
</table>
Support for tagging rules in a SIP profile configuration

This feature allows users to tag the rules in a SIP profile configuration. Tagging the rules allows users to insert or delete rules at any position of the existing SIP profile configuration without deleting and reconfiguring the entire voice-class sip profile.

The following command is introduced in voice class sip profiles configuration mode to tag and insert rules: `rule`

This feature also allows users to upgrade or downgrade all the existing SIP profile configurations to rule-format and non-rule format.

The following commands are introduced in global configuration mode: `voice sip sip-profiles upgrade`, `voice sip sip-profiles downgrade`

---

### Information About SIP Profiles

Protocol translation and repair is a key Cisco Unified Border Element (CUBE) function. CUBE can be deployed between two devices that support the same VoIP protocol (for example, SIP), but do not interwork because of differences in how the protocol is implemented or interpreted. CUBE can customize the SIP messaging on either side to what the devices in that segment of the network expects to see by normalizing the SIP messaging on the network border, or between two non-interoperable devices within the network.

Service providers may have policies for which SIP messaging fields should be present (or what constitutes valid values for the header fields) 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 8: SIP Profile

In order to customize SIP messaging in both directions, you can place and configure a CUBE with a SIP profile at the boundary of these networks.

In addition to network policy compliance, the CUBE SIP profiles can be used to resolve incompatibilities between SIP devices inside the enterprise network. These are 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.

**Important Characteristics of SIP Profiles**

Given below are a few important notes for SIP Profiles:

• Copy Variables u01 to u99 are shared by inbound and outbound 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 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 is 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 need to press "Ctrl+v" keys and then type '?'. This is needed to treat '?' as an input character itself instead of usual device help prompt.

• 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 occurs, a back slash must prefix the double quotes. For example, “User-Agent: \"CISCO\" CUBE”
  * Regular expressions are supported.

Inbound SIP Profile:

• If the incoming message contains multiple instances of 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 dial peers are 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 for SIP Profiles

• 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.

• Syntax checking is not performed on SIP messages after SIP profile rules have been applied. Changes 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, 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.

• We cannot modify the "image" m-line attributes (m=image 16850 udptl t38) 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.

• Existing 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 vice-versa.

How to Configure SIP Profiles

To configure SIP Profiles, you must first configure the SIP Profile globally, and apply it at either to all dial peers (globally) or to a single dial peer (dial-peer level). After a SIP profile is configured, it can be applied as an inbound or outbound profile.
Configuring 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:
   - request message {sip-header | sdp-header} header-to-add add header-value-to-add
   - request message {sip-header | sdp-header} header-to-remove remove
   - 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:
   - response message [method method-type] {sip-header | sdp-header} header-to-add add header-value-to-add
   - response message [method method-type] {sip-header | sdp-header} header-to-remove remove
   - 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 voice class sip-profiles profile-id</td>
<td>Creates a SIP Profiles and enters voice class configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# voice class sip-profiles 10</td>
<td></td>
</tr>
<tr>
<td>Step 4 Enter one of the following to add, remove, modify SIP headers:</td>
<td>According to your choice, this step does one of the following:</td>
</tr>
<tr>
<td>• request message {sip-header</td>
<td>sdp-header} header-to-add add header-value-to-add</td>
</tr>
<tr>
<td>• request message {sip-header</td>
<td>sdp-header} header-to-remove remove</td>
</tr>
<tr>
<td></td>
<td>• Modifies a SIP or SDP header to a SIP request.</td>
</tr>
</tbody>
</table>
Configuring SIP Profile Using Rule Tag

Configure SIP profile rules using the rule tag, enables you to performing the following tasks:

- Add SIP profile request and response headers with a rule tag.
- Modify the existing SIP profile configurations by inserting a rule at any position of the SIP profile without deleting and reconfiguring the entire SIP profile.
- Remove a rule by specifying only rule tag.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| • request message {sip-header | sdp-header} header-to-modify modify header-value-to-match header-value-to-replace | • If ANY is used in place of a header, it indicates that a rule must be applied to any message within the specified category.  
• For header-value-to-add used to add a header, header-value-to-match or header-value-to-replace used to modify a header:  
  * If a whitespace occurs, the entire value must be included between double quotes. For example, ”User-Agent: CISCO CUBE”  
  * If double quotes occurs, a back slash must prefix the double quotes. For example, ”User-Agent: \"CISCO\" CUBE”  
  * Regular expressions are supported. |

**Step 5**
Enter one of the following to add, remove, or modify SIP response headers:

- • response message [method method-type] {sip-header | sdp-header} header-to-add add header-value-to-add
- • response message [method method-type] {sip-header | sdp-header} header-to-remove remove
- • 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:

- Adds a SIP or SDP header to a SIP response.
- Removes a SIP or SDP header to a SIP response.
- Modifies a SIP or SDP header to a SIP response.
- All notes from the previous step are applicable here.

**Step 6**
end

Exits to privileged EXEC mode
Below are the rule tag behaviors that need to be considered while using rule tag in SIP profile configurations:

- 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 non-rule format, upgrade the SIP profiles to rule format before inserting a rule.
- If a new rule is inserted, the new rule takes the position specified in `before tag`. The subsequent rules are incremented sequentially.
- Once the rule is removed, the tag belonging to the removed rule remains vacant. The tags 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.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice class sip-profiles profile-id`
4. Enter one of the following to add, copy, modify, or remove a SIP request or response headers to a SIP profile configuration:
   
   - `rule tag request method sdp-header | sip-header header-name add|copy|modify|remove string`
   - `rule tag response method sdp-header | sip-header header-name add|copy|modify|remove string`
5. Enter one of the following to insert a rule in between the existing set of rules to add, remove, or modify SIP request or response headers:
   
   - `rule before tag request method sdp-header | sip-header header-name add|copy|modify|remove string`
   - `rule before tag response method sdp-header | sip-header header-name add|copy|modify|remove string`
6. Enter the following to delete a rule:
   
   - `no rule tag`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>voice class sip-profiles profile-id</th>
</tr>
</thead>
</table>

**Example:**

Device(config)# voice class sip-profiles 10

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a SIP Profile and enters voice class configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Enter one of the following to add, copy, modify, or remove a SIP request or response headers to a SIP profile configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• rule tag request method sdp-header</td>
</tr>
<tr>
<td></td>
<td>header-name add</td>
</tr>
<tr>
<td></td>
<td>• rule tag response method sdp-header</td>
</tr>
<tr>
<td></td>
<td>header-name add</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>According to your choice, this step tags the SIP request or response header with a unique number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Enter one of the following to insert a rule in between the existing set of rules to add, remove, or modify SIP request or response headers:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• rule before tag request method sdp-header</td>
</tr>
<tr>
<td></td>
<td>header-name add</td>
</tr>
<tr>
<td></td>
<td>• rule before tag response method sdp-header</td>
</tr>
<tr>
<td></td>
<td>sip-header header-name add</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>According to your choice this steps inserts the rule at the position specified in the <strong>before</strong> tag. The subsequent rules in the existing SIP profile configuration is incremented sequentially.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Enter the following to delete a rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• no rule tag</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>According to your choice, this step tags the SIP request or response with a unique number.</td>
</tr>
</tbody>
</table>

| Step 7 | end |

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exits voice class sip-profiles configuration mode.</td>
</tr>
</tbody>
</table>
Configuring a SIP Profile for Non-standard SIP 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:
   - `request message {sip-header} {non-standard-header-to-add add non-standard-header-value-to-add}
   - `request message {sip-header} {non-standard-header-to-copy copy non-standard-header-value-to-match copy-variable`
   - `request message {sip-header} {non-standard-header-to-remove remove`
   - `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:
   - `response message [method method-type] {sip-header} {non-standard-header-to-remove remove`

6. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** voice class sip-profiles profile-id | Creates a SIP Profiles and enters voice class configuration mode.  
Example:  
Device(config)# voice class sip-profiles 10 |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter one of the following to add, copy, remove, or modify non-standard SIP request headers:</td>
</tr>
</tbody>
</table>
| • `request message {sip-header}`
  `non-standard-header-to-add add`
  `non-standard-header-value-to-add` | According to your choice, this step does one of the following: |
| • `request message {sip-header}`
  `non-standard-header-to-copy copy`
  `non-standard-header-value-to-match copy-variable` | • Adds a non-standard SIP header to a SIP request. |
| • `request message {sip-header}`
  `non-standard-header-to-remove remove` | • Copies contents from a non-standard SIP header to a SIP request. |
| • `request message {sip-header}`
  `non-standard-header-to-modify modify`
  `non-standard-header-value-to-match`
  `non-standard-header-value-to-replace` | • Removes a non-standard SIP header to a SIP request. |
| • If ANY is used in place of a header, it indicates that a rule must be applied to any message within the specified category. |
| • For `non-standard-header-value-to-add` used to add a non-standard header, `non-standard-header-value-to-match` or `non-standard-header-value-to-replace` used to modify a non-standard header: |
| ◦ If a whitespace occurs, the entire value must be included between double quotes. For example, "User-Agent: CISCO CUBE" | • Modifies a non-standard SIP header to a SIP request. |
| ◦ If double quotes occurs, a back slash must prefix the double quotes. For example, "User-Agent: "CISCO" CUBE" | • Regular expressions are supported. |
| **Step 5** | Enter one of the following to add, copy, remove, or modify non-standard SIP response headers: |
| • `response message [method method-type] {sip-header}`
  `non-standard-header-to-add add`
  `non-standard-header-value-to-add` | According to your choice, this step does one of the following: |
| • `response message [method method-type] {sip-header}`
  `non-standard-header-to-copy copy`
  `non-standard-header-value-to-match copy-variable` | • Adds a non-standard SIP to a SIP response. |
| • `response message [method method-type] {sip-header}`
  `non-standard-header-to-remove remove` | • Copies contents from a non-standard SIP header to a SIP response. |
| • `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` | • Removes a non-standard header to a SIP response. |
| • All notes from the previous step are applicable here. | • Modifies a non-standard SIP header to a SIP response. |

### Upgrading or Downgrading SIP Profile Configurations

You can upgrade or downgrade all the SIP Profile configurations to rule-format or non-rule format automatically.

**Note**: We recommend that you downgrade the SIP profiles to non-rule format configuration before migrating to a version below Cisco IOS Release 15.5(2)T or Cisco IOS-XE Release 3.15S. If you migrate without downgrading the SIP profile configurations, then all the SIP profile configurations is lost after migration.

#### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code> Exits to privileged EXEC mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code> Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enter the following to upgrade SIP profiles configurations to rule-format:</td>
</tr>
<tr>
<td></td>
<td>• <code>voice sip sip-profiles upgrade</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter the following to downgrade SIP profiles configurations to non-rule format:</td>
</tr>
<tr>
<td></td>
<td>• <code>voice sip sip-profiles downgrade</code></td>
</tr>
</tbody>
</table>
Configuring 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

DETAILLED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 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 | | 

Example:
In dial-peer configuration mode

```
!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
```

Example:
Configuring a SIP Profile as an Inbound Profile

You can configure a SIP profile as an inbound profile applied globally or to a single inbound dial peer. Inbound SIP profiles feature must be enabled before applying it to dial peers.

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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 | Enters global VoIP configuration mode. |
  
**Example:**

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

**Command or Action** | **Purpose**
--- | ---
**Step 4** | **sip**

**Example:**

```
Device(config-voi-serv)# sip
```

Enters global VoIP SIP configuration mode.

**Step 5** | **sip-profiles inbound**

**Example:**

```
Device(config-voi-sip)# sip-profiles inbound
```

Enables inbound SIP profiles feature.

**Step 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

**Example:**

In dial-peer configuration mode

```
!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
```

**Example:**

In global VoIP SIP mode

```
! 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
```

**Step 7** | **end**

Exits to privileged EXEC mode

---

**Verifying SIP Profiles**

**SUMMARY STEPS**

1. `show dial-peer voice id | include profile`
SIP Profiles

Troubleshooting SIP Profiles

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 profile

Translation profile (Incoming):
Translation profile (Outgoing):
translation-profile = '
voice class sip profiles = 11
voice class sip profiles inbound = 10

Troubleshooting SIP Profiles

SUMMARY STEPS

1. debug ccsip all

DETAILED STEPS

ddebug 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 performed by the SIP profile configuration, by preceding the modification information with the word sip_profiles, as highlighted in the example below.

Example:
Device# debug ccsip all

...  
Oct 12 06:51:53.647: //1/xxxxxxxxxxxx/SIP/Info/
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
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

Applying the SIP Profiles

! Applying SIP profiles globally
Device(config)# voice service voip
Device (config-voi-serv) sip-profiles 20
Device (config-voi-serv) end

! 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) voice-class sip profiles 40
Device (config-dial-peer) voice-class sip profiles 10
Device (config-dial-peer) 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 "(.*:\(.*\))" "\gateway@"

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 "(.*:\(.*\))" "\gateway@"

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>"

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"

Applying the SIP Profiles to Dial Peers

! Applying SIP Profiles globally
Device(config)# voice service voip
Device (config-voi-serv) sip-profiles 20
Device (config-voi-serv) sip-profiles 10
Device (config-voi-serv) sip-profiles 103
Device (config-voi-serv) sip-profiles 30
Device (config-voi-serv) exit

! Applying SIP Profiles to one dial peer only
Device (config) dial-peer voice 90 voip
Device (config-dial-peer) voice-class sip profiles 30

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: 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

Before upgrading a SIP Profile

Device# voice class sip-profiles 1
Device# request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
Device# request INVITE sip-header Supported Add "Supported: "
Device# voice sip sip-profiles upgrade

After Upgrading a SIP Profile

Device# voice class sip-profiles 1
Device# rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
Device# rule 2 request INVITE sip-header Supported Add "Supported: "

Downgrading SIP Profiles

Before downgrading a SIP Profile

Device# voice class sip-profiles 1
Device# rule 1 request INVITE sip-header Contact Modify "(.*)" "\1;temp=xyz"
Device# rule 2 request INVITE sip-header Supported Add "Supported: "
Device# voice sip sip-profiles downgrade
After downgrading a SIP Profile

Device(config)# voice class sip-profiles 1
Device(config-class)# request INVITE sip-header Contact Modify "(.*)" ";\l;temp=xyz"
Device(config-class)# request INVITE sip-header Supported Add "Supported: ">

Example: Modifying Diversion Headers

Example: Modify Diversion Headers from Three-Digit Extensions to Ten Digits.

Most 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
```

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.

Example: Sample SIP Profile Application on SIP Invite Message

The SIP profile configured is 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" ";-"
```

The SIP INVITE message before the SIP profile has been applied is show below:

```
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=F11AEQ1-1D8D
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=F11AEQ1-1D8D
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**

Prior to Cisco IOS Release 15.5(2)T, there was no method to add, copy, delete, or modify any non-standard SIP headers like 'X-Cisco-Recording-Participant' using SIP profiles. The SIP profile will look for the new option "WORD" that allows the user to change any non-standard 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
```
Session Refresh with Reinvites

- Finding Feature Information, page 237
- Prerequisites for Session Refresh with Reinvites, page 237
- Information about Session Refresh with Reinvites, page 238
- How to Configure Session Refresh with Reinvites, page 238
- Feature Information for Session Refresh with Reinvites, page 240

Finding Feature Information

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

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

Prerequisites for Session Refresh with Reinvites

The allow-connections sip to sip command must be configured before you configure the Session refresh with Reinvites feature. For more information and configuration steps see the "Configuring SIP-to-SIP Connections in a Cisco Unified Border Element" section.

Cisco Unified Border Element

- Cisco IOS Release 12.4(20)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Information about Session Refresh with Reinvites

Configuring support for session refresh with reinvites expands the ability of the Cisco Unified Border Element to receive a REINVITE message that contains either a session refresh parameter or a change in media via a new SDP and ensure the session does not time out. The midcall-signaling command distinguishes between the way a Cisco Unified Communications Express and Cisco Unified Border Element releases signaling messages. Most SIP-to-SIP video and SIP-to-SIP ReInvite-based supplementary services features require the Configuring Session Refresh with Reinvites feature to be configured.

Cisco IOS Release 12.4(15)XZ and Earlier Releases
Session refresh support via OPTIONS method. For configuration information, see the "Enabling In-Dialog OPTIONS to Monitor Active SIP Sessions" section.

Cisco IOS Release 12.4(15)XZ and Later Releases
Cisco Unified BE transparently passes other session refresh messages and parameters so that UAs and proxies can establish keepalives on a call.

How to Configure Session Refresh with Reinvites

Configuring Session refresh with Reinvites

Before You Begin

Note
SIP-to-SIP video calls and SIP-to-SIP ReInvite-based supplementary services fail if the midcall-signaling command is not configured.

Note
The following features function if the midcall-signaling command is not configured: session refresh, fax, and refer-based supplementary services.

- Configuring Session Refresh with Reinvites is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the midcall-signaling command be configured
- Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.
## SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. midcall-signaling passthru
6. exit
7. end

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| Example: Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Router# configure terminal |
| **Step 3** voice service voip | Enters VoIP voice-service configuration mode. |
| Example: Router(config)# voice service voip |
| **Step 4** sip | Enters SIP configuration mode. |
| Example: Router(conf-voi-serv)# sip |
| **Step 5** midcall-signaling passthru | Passes SIP messages from one IP leg to another IP leg. |
| Example: Router(conf-serv-sip)# midcall-signaling passthru |
| **Step 6** exit | Exits the current mode. |
| Example: Router(conf-serv-sip)# exit |
## Feature Information for Session Refresh with Reinvites

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Refresh with Reinvites</td>
<td>12.4(20)T</td>
<td>Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS Release 12.4(20)T, this feature was implemented on the Cisco Unified Border Element. midcall-signaling</td>
</tr>
<tr>
<td>Session Refresh with Reinvites</td>
<td>Cisco IOS XE Release 2.5</td>
<td>Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS XE Release 2.5, this feature was implemented on the Cisco Unified Border Element (Enterprise). midcall-signaling</td>
</tr>
</tbody>
</table>
CHAPTER 24

SIP Stack Portability

Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses.

- Finding Feature Information, page 241
- Prerequisites for SIP Stack Portability, page 241
- Information About SIP Stack Portability, page 242
- SIP Call-Transfer Basics, page 242
- Feature Information for SIP Stack Portability, page 253

Finding Feature Information

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

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

Prerequisites for SIP Stack Portability

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(2)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

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

The SIP Stack Portability feature implements the following capabilities to the Cisco IOS SIP gateway stack:

- It receives inbound Refer message requests both within a dialog and outside of an existing dialog from the user agents (UAs).
- It sends and receives SUBSCRIBE or NOTIFY message requests via UAs.
- It receives unsolicited NOTIFY message requests without having to subscribe to the event that was generated by the NOTIFY message request.
- It supports outbound delayed media.

It sends an INVITE message request without Session Description Protocol (SDP) and provides SDP information in either the PRACK or ACK message request for both initial call establishment and mid-call re-INVITE message requests.

- It sets SIP headers and content body in requests and responses.

The stack applies certain rules and restrictions for a subset of headers and for some content types (such as SDP) to protect the integrity of the stack's functionality and to maintain backward compatibility. When receiving SIP message requests, it reads the SIP header and any attached body without any restrictions.

To make the best use of SIP call-transfer features, you should understand the following concepts:

SIP Call-Transfer Basics

Basic Terminology of SIP Call Transfer

Call transfer allows a wide variety of decentralized multiparty call operations. These decentralized call operations form the basis for third-party call control, and thus are important features for VoIP and SIP. Call transfer is also critical for conference calling, where calls can transition smoothly between multiple point-to-point links and IP-level multicasting.

Refer Message Request

The SIP Refer message request provides call-transfer capabilities to supplement the SIP BYE and ALSO message requests already implemented on Cisco IOS SIP gateways. The Refer message request has three main roles:

- Originator--User agent that initiates the transfer or Refer request.
- Recipient--User agent that receives the Refer request and is transferred to the final-recipient.
- Final-Recipient--User agent introduced into a call with the recipient.

Note

A gateway can be a recipient or final recipient, but not an originator.
The Refer message request always begins within the context of an existing call and starts with the *originator*. The originator sends a Refer request to the *recipient* (user agent receiving the Refer request) to initiate a triggered INVITE request. The triggered INVITE request uses the SIP URL contained in the Refer-To header as the destination of the INVITE request. The recipient then contacts the resource in the Refer-To header (*final recipient*), and returns a SIP 202 (Accepted) response to the originator. The recipient also must notify the originator of the outcome of the Refer transaction—whether the final recipient was successfully contacted or not. The notification is accomplished using the SIP NOTIFY message request, SIP’s event notification mechanism. A NOTIFY message with a message body of SIP 200 OK indicates a successful transfer, and a message body of SIP 503 Service Unavailable indicates an unsuccessful transfer. If the call was successful, a call between the recipient and the final recipient results.

The figure below represents the call flow of a successful Refer transaction initiated within the context of an existing call.

**Figure 9: Successful Refer transaction**

<table>
<thead>
<tr>
<th>Originator</th>
<th>Recipient</th>
<th>Final recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>user agent A</td>
<td>user agent B</td>
<td>user agent C</td>
</tr>
</tbody>
</table>

**INVITE/200/ACK**

2-Way RTP

Refer: Refer-To: Agent C

202 Accepted

Notify (100 Trying body)

200 OK

Refer-To Header

The recipient receives from the originator a Refer request that always contains a single Refer-To header. The Refer-To header includes a SIP URL that indicates the party to be invited and must be in SIP URL format.

---

**Note**

The TEL URL format cannot be used in a Refer-To header, because it does not provide a host portion, and without one, the triggered INVITE request cannot be routed.

The Refer-To header may contain three additional overloaded headers to form the triggered INVITE request. If any of these three headers are present, they are included in the triggered INVITE request. The three headers are:
Basic Terminology of SIP Call Transfer

- **Accept-Contact--Optional in a Refer request.** A SIP Cisco IOS gateway that receives an INVITE request with an Accept-Contact does not act upon this header. This header is defined in draft-ietf-sip-callerprefs-03.txt and may be used by user agents that support caller preferences.

- **Proxy-Authorization--Nonstandard header that SIP gateways do not act on.** It is echoed in the triggered INVITE request because proxies occasionally require it for billing purposes.

- **Replaces--Header used by SIP gateways to indicate whether the originator of the Refer request is requesting a blind or attended transfer.** It is required if the originator is performing an attended transfer, and not required for a blind transfer.

All other headers present in the Refer-To are ignored, and are not sent in the triggered INVITE.

---

**Note**

The Refer-To and Contact headers are required in the Refer request. The absence of these headers results in a 4xx class response to the Refer request. Also, the Refer request must contain exactly one Refer-To header. Multiple Refer-To headers result in a 4xx class response.

---

**Referred-By Header**

The Referred-By header is required in a Refer request. It identifies the originator and may also contain a signature (included for security purposes). SIP gateways echo the contents of the Referred-By header in the triggered INVITE request, but on receiving an INVITE request with this header, gateways do not act on it.

---

**Note**

The Referred-By header is required in a Refer request. The absence of this header results in a 4xx class response to the Refer request. Also, the Refer request must contain exactly one Referred-By header. Multiple Referred-By headers result in a 4xx class response.

---

**NOTIFY Message Request**

Once the outcome of the Refer transaction is known, the recipient of the Refer request must notify the originator of the outcome of the Refer transaction--whether the final-recipient was successfully contacted or not. The notification is accomplished using the NOTIFY message request, SIP’s event notification mechanism. The notification contains a message body with a SIP response status line and the response class in the status line indicates the success or failure of the Refer transaction.

The NOTIFY message must do the following:

- Reflect the same To, From, and Call-ID headers that were received in the Refer request.
- Contain an Event header refer.
- Contain a message body with a SIP response line. For example: SIP/2.0 200 OK to report a successful Refer transaction, or SIP/2.0 503 Service Unavailable to report a failure. To report that the recipient disconnected before the transfer finished, it must use SIP/2.0 487 Request Canceled.

Two Cisco IOS commands pertain to the NOTIFY message request:

- The `timers notify` command sets the amount of time that the recipient should wait before retransmitting a NOTIFY message to the originator.
Types of SIP Call Transfer Using the Refer Message Request

This section discusses how the Refer message request facilitates call transfer. There are two types of call transfer: blind and attended. The primary difference between the two is that the Replaces header is used in attended call transfers. The Replaces header is interpreted by the final recipient and contains a Call-ID header, indicating that the initial call leg is to be replaced with the incoming INVITE request.

As outlined in the Refer message request, there are three main roles:

- Originator--User agent that initiates the transfer or Refer request.
- Recipient--User agent that receives the Refer request and is transferred to the final recipient.
- Final-Recipient--User agent introduced into a call with the recipient.

A gateway can be a recipient or final recipient, but not an originator.

Blind Call-Transfer Process

A blind, or unattended, transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. This is different from a consultative, or attended, transfer in which one of the transferring parties either connects the caller to a ringing phone (ringback heard) or speaks with the third party before connecting the caller to the third party. Blind transfers are often preferred by automated devices that do not have the capability to make consultation calls.

Blind transfer works as described in the Types of SIP Call Transfer Using the Refer Message Request, on page 245. The process is as follows:

1. Originator (user agent that initiates the transfer or Refer request) does the following:
   1. Sets up a call with recipient (user agent that receives the Refer request)
   2. Issues a Refer request to recipient

2. Recipient does the following:
   1. Sends an INVITE request to final recipient (user agent introduced into a call with the recipient)
   2. Returns a SIP 202 (Accepted) response to originator
   3. Notifies originator of the outcome of the Refer transaction--whether final recipient was successfully contacted or not (SIP 503 Service Unavailable)

3. If successful, a call is established between recipient and final recipient.

4. The original signaling relationship between originator and recipient terminates when either of the following occurs:

5. One of the parties sends a Bye request.
Recipient sends a Bye request after successful transfer (if originator does not first send a Bye request after receiving an acknowledgment for the NOTIFY message).

The figure below shows a successful blind or unattended call transfer in which the originator initiates a Bye request to terminate signaling with the recipient.

**Figure 10: Successful Blind or Unattended Transfer--Originator Initiating a Bye Request**
The figure below shows a successful blind or unattended call transfer in which the recipient initiates a Bye request to terminate signaling with the originator. A NOTIFY message is always sent by the recipient to the originator after the final outcome of the call is known.

Figure 11: Successful Blind or Unattended Transfer--Recipient Initiating a Bye Request

1. Originator sends a re-INVITE that takes the call off hold and returns to the original call with recipient.
2. Final recipient sends an 18x informational response to recipient.
3. The call fails; the originator cannot recover the call with recipient. Failure can be caused by an error condition or timeout.
4. The call leg between originator and recipient remains active (see the figure below).
5. If the INVITE to final recipient fails (408 Request Timeout), the following occurs:
   1. Recipient notifies originator of the failure with a NOTIFY message.
Originator sends a re-INVITE and returns to the original call with the recipient.

**Figure 12: Failed Blind Transfer--Originator Returns to Original Call with Recipient**

**Attended Transfer**

In attended transfers, the Replaces header is inserted by the initiator of the Refer message request as an overloaded header in the Refer-To and is copied into the triggered INVITE request sent to the final recipient. The header has no effect on the recipient, but is interpreted by the final recipient as a way to distinguish between blind transfer and attended transfer. The attended transfer process is as follows:

1. Originator does the following:
   1. Sets up a call with recipient.
   2. Places recipient on hold.
   3. Establishes a call to final recipient.
   4. Sends recipient a Refer message request with an overloaded Replaces header in the Refer-To header.

2. Recipient does the following:
   1. Sends a triggered INVITE request to final recipient. (Request includes the Replaces header, identifying the call leg between the originator and the final recipient.)
2 Recipient returns a SIP 202 (Accepted) response to originator. (Response acknowledges that the INVITE has been sent.)

3 Final recipient establishes a direct signaling relationship with recipient. (Replaces header indicates that the initial call leg is to be shut down and replaced by the incoming INVITE request.)

4 Recipient notifies originator of the outcome of the Refer transaction. (Outcome indicates whether or not the final recipient was successfully contacted.)

5 Recipient terminates the session with originator by sending a Bye request.

Replaces Header

The Replaces header is required in attended transfers. It indicates to the final recipient that the initial call leg (identified by the Call-ID header and tags) is to be shut down and replaced by the incoming INVITE request. The final recipient sends a Bye request to the originator to terminate its session.

If the information provided by the Replaces header does not match an existing call leg, or if the information provided by the Replaces header matches a call leg but the call leg is not active (a Connect, 200 OK to the INVITE request has not been sent by the final-recipient), the triggered INVITE does not replace the initial call leg and the triggered INVITE request is processed normally.

Any failure resulting from the triggered INVITE request from the recipient to the final recipient does not drop the call between the originator and the final recipient. In these scenarios, all calls that are active (originator to recipient and originator to final recipient) remain active after the failed attended transfer attempt.
The figure below shows a call flow for a successful attended transfer.

**Figure 13: Successful Attended Transfer**

<table>
<thead>
<tr>
<th>Orignator</th>
<th>Recipient</th>
<th>Final recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE:200/ACK</td>
<td>Call ID:1:from_tag11:to_tag22</td>
<td></td>
</tr>
<tr>
<td>2-Way RTP</td>
<td>Invite (hold) Call ID:1:from_tag11:to_tag22</td>
<td></td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ack Call ID:1:from_tag11:to_tag22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite Call ID:2:from_tag33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK Call ID:2:from_tag33:to_tag44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ack Call ID:2:from_tag33:to_tag44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refer:Refer-To:&lt;final-recipient&gt;replaces: Call ID:2:from_tag33:to_tag44 &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call ID:1:from_tag11:to_tag22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Accepted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notify (100 Trying body)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 Trying</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite Call ID:3:from_tag55 FLAGS: replaces: Call ID:2:from_tag33:to_tag44 &gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notify [200] Call ID:1:from_tag11:to_tag22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK Call ID:3:from_tag55:to_tag66</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK (Notify)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ByCe:Call ID:1:from_tag11:to_tag22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK (Bye)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-Way RTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bye Call ID:2:from_tag33:to_tag44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK (Bye)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Attended Transfer with Early Completion**

Attended transfers allow the originator to have a call established between both the recipient and the final recipient. With attended transfer with early completion, the call between the originator and the final recipient does not have to be active, or in the talking state, before the originator can transfer it to the recipient. The
originator establishes a call with the recipient and only needs to be setting up a call with the final recipient. The final recipient may be ringing, but has not answered the call from the originator when it receives a re-INVITE to replace the call with the originator and the recipient.

The process for attended transfer with early completion is as follows (see the figure below):

1. Originator does the following:
   1. Sets up a call with recipient.
   2. Places the recipient on hold.
   3. Contacts the final recipient.
   4. After receiving an indication that the final recipient is ringing, sends recipient a Refer message request with an overloaded Replaces header in the Refer-To header. (The Replaces header is required in attended transfers and distinguishes between blind transfer and attended transfers.)

2. Recipient does the following:
   1. Returns a SIP 202 (Accepted) response to the originator. (to acknowledge that the INVITE has been sent.)
   2. Upon receipt of the Refer message request, sends a triggered INVITE request to final recipient. (The request includes the Replaces header, which indicates that the initial call leg, as identified by the Call-ID header and tags, is to be shut down and replaced by the incoming INVITE request.)

3. Final recipient establishes a direct signaling relationship with recipient.

4. Final recipient tries to match the Call-ID header and the To or From tag in the Replaces header of the incoming INVITE with an active call leg in its call control block. If a matching active call leg is found, final recipient replies with the same status as the found call leg. However, it then terminates the found call leg with a 487 Request Cancelled response.

**Note**

If early transfer is attempted and the call involves quality of service (QoS) or Resource Reservation Protocol (RSVP), the triggered INVITE from the recipient with the Replaces header is not processed and the transfer fails. The session between originator and final recipient remains unchanged.

1. Recipient notifies originator of the outcome of the Refer transaction--that is, whether final recipient was successfully contacted or not.
Recipient or originator terminates the session by sending a Bye request.

**Figure 14: Attended Transfer with Early Completion**

<table>
<thead>
<tr>
<th>Orignator</th>
<th>Recipient</th>
<th>Final recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE/200/ACK&lt;br&gt;Call-id:1; from-tag:11; to-tag:22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-way RTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVITE(hold)/200/ACK&lt;br&gt;Call-id:1; from-tag:11; to-tag:22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTP on hold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invite Call-id:2; from-tag:33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18x Call-id:2; from-tag:33; to-tag:44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete transfer early</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refer (Refer-To: final-recipient? Replaces Call-id:2; from-tag:33; to-tag:44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call-id:1; from-tag: to-tag:22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP 200 Accepted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notify (100 Trying body)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Invite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>100 Trying</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Invite Call-id:3; from-tag:55</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Replaces: Call-id:2; from-tag:33; to-tag:44</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18x Call-id:3; from-tag:55; to-tag:66</td>
<td></td>
</tr>
<tr>
<td>487 Request Cancelled Call-id:2; from-tag:33; to-tag:44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 OK Call-id:3; from-tag:55; to-tag:66</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTIYI: 200 OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Call-id: from-tag:11; to-tag:22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYE/200 OK&lt;br&gt;Call-id:1; from-tag:11; to-tag:22</td>
<td></td>
</tr>
</tbody>
</table>

**VSA for Call Transfer**

You can use a vendor-specific attribute (VSA) for SIP call transfer.

**Referred-By Header**

For consistency with existing billing models, Referred-By and Requested-By headers are populated in call history tables as a VSA. Cisco VSAs are used for VoIP call authorization. The new VSA tag
supp-svc-xfer-by helps to associate the call legs for call-detail-record (CDR) generation. The call legs can be originator-to-recipient or recipient-to-final-recipient.

The VSA tag supp-svc-xfer-by contains the user@host portion of the SIP URL of the Referred-By header for transfers performed with the Refer message request. For transfers performed with the Bye/Also message request, the tag contains user@host portion of the SIP URL of the Requested-By header. For each call on the gateway, two RADIUS records are generated: start and stop. The supp-svc-xfer-by VSA is generated only for stop records and is generated only on the recipient gateway—the gateway receiving the Refer or Bye/Also message.

The VSA is generated when a gateway that acts as a recipient receives a Refer or Bye/Also message with the Referred-By or Requested-By headers. There are usually two pairs of start and stop records. There is a start and stop record between the recipient and the originator and also between the recipient to final recipient. In the latter case, the VSA is generated between the recipient to the final recipient only.

Business Group Field

A new business group VSA field has been added that assists service providers with billing. The field allows service providers to add a proprietary header to call records. The VSA tag for business group ID is cust-biz-grp-id and is generated only for stop records. It is generated when the gateway receives an initial INVITE with a vendor dial-plan header to be used in call records. In cases when the gateway acts as a recipient, the VSA is populated in the stop records between the recipient and originator and the final recipient.

Note

For information on VSAs, see the RADIUS VSA Voice Implementation Guide.

Feature Information for SIP Stack Portability

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 Stack Portability

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Stack Portability</td>
<td>Cisco IOS XE Release 2.5</td>
<td>Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses. The following commands were introduced or modified: None</td>
</tr>
</tbody>
</table>
### Feature Information for SIP Stack Portability

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Stack Portability</td>
<td>12.4(2)T</td>
<td>Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses. The following commands were introduced or modified: <strong>None</strong></td>
</tr>
</tbody>
</table>
VoIP for IPv6

This document describes VoIP in IPv6 (VoIPv6), a feature that adds IPv6 capability to existing VoIP features. This feature adds dual-stack (IPv4 and IPv6) support on voice gateways and media termination points (MTPs), IPv6 support for Session Initiation Protocol (SIP) trunks, and support for Skinny Client Control Protocol (SCCP)-controlled analog voice gateways. In addition, the Session Border Controller (SBC) functionality of connecting a SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on a Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.

- Finding Feature Information, page 255
- Prerequisites for VoIP for IPv6, page 256
- Restrictions for Implementing VoIP for IPv6, page 256
- Information About VoIP for IPv6, page 257
- How to Configure VoIP for IPv6, page 264
- Configuration Examples for VoIP over IPv6, page 290
- Troubleshooting Tips for VoIP for IPv6, page 290
- Verifying and Troubleshooting Tips, page 291
- Feature Information for VoIP for IPv6, page 307

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for VoIP for IPv6

- Cisco Express Forwarding for IPv6 must be enabled.
- Virtual routing and forwarding (VRF) is not supported in IPv6 calls.

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)T or a later release must be installed and running on your Cisco UBE.

Cisco Unified Border Element (Enterprise)

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

Restrictions for Implementing VoIP for IPv6

The following are the restrictions for Cisco UBE features:

Media Flow—Through

- Video call flows with Alternative Network Address Types (ANAT) are not supported.
- WebEx call flow with ANAT are not supported (Cisco UBE does not support ANAT on Video and Application media types).

SDP Pass-Through

- Supports only Early Offer (EO)—Early Offer (EO) and Delayed Offer (DO)—Delayed Offer (DO) call flows.
- Delayed Offer—Early Offer call flow falls back to Delayed Offer—Delayed Offer call flow.
- Supplementary services are not supported on SDP Pass-Through.
- Transcoding and DTMF interworking are not supported.

Note

The above SDP Pass—Through restrictions are applicable for both IPv4 and IPv6.

- SDP Pass—Through does not support the dual-stack functionality.
- ANAT call flows does not support IPv4-to-IPv6 and IPv6-to-IPv4 Media interworking.

UDP Checksum

- CEF and process options are not supported on ASR1000 series routers.
- None option is partially supported on ISR–G2.
Media Anti–Trombone

- Media Anti–Trombone is not enabled if the initial call before tromboning is in Flow–Around (FA) mode.
- Media Anti–Trombone supports only symmetric media address type interworking (IPv4-IPv4 or IPv6-IPv6 media) with or without ANAT.
- Does not provide support for IPv4-IPv6 interworking cases with or without ANAT because Cisco UBE cannot operate in FA mode post tromboning.

Information About VoIP for IPv6

SIP Features Supported on IPv6

The Session Initiation Protocol (SIP) is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP.

The Cisco SIP functionality enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. SIP features also provide advantages in the following areas:

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

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.

Dual-stack SIP UAs use Alternative Network Address Transport (ANAT) grouping semantics:

- Includes both IPv4 and IPv6 addresses in the Session Description Protocol (SDP).
- Is automatically enabled in dual-stack mode (can be disabled if required).
- Requires media to be bound to an interface that have both IPv4 and IPv6 addresses.
- Described in RFC 4091 and RFC 4092 (RFC 5888 describes general SDP grouping framework).

SIP UAs use "sdp-anat" option tag in the Required and Supported SIP header fields:

- Early Offer (EO) INVITE using ANAT semantics places "sdp-anat" in the Require header.
- Delayed Offer (DO) INVITE places "sdp-anat" in the Supported header.

SIP Signaling and Media Address Selection:

- Source address for SIP signaling is selected based on the destination signaling address type configured in the session-target of the outbound dial-peer.
If signaling bind is configured, source SIP signaling address is chosen from the bound interface.

If signaling bind is not configured, source SIP signaling address is chosen based on the best address in the UA to reach the destination signaling address.

SDP may or may not use ANAT semantics:

- When ANAT is used, media addresses in SDP are chosen from the interface media that is configured.
- When ANAT is not used, media addresses in SDP are chosen based on the best address to reach the destination signaling address (when no media bind is configured).

### SIP Voice Gateways in VoIPv6

Session Initiation Protocol (SIP) is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

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 new calls 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 rejected requires to be checked for the show commands to be consistent before and after the switchover.

  For more information, refer to the "Support for 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 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 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.
• **SIP VMWI for FXS phones**: SIP provides visible message waiting indication (VMWI) on FXS phones. This feature provides users with the option to enable one message waiting indication (MWI): audible, visible, or both. The VMWI mechanism uses SIP Subscribe or Notify to get MWI updates from a virtual machine (VM) system, and then forwards updates to the FXS phone on the port.

For more information, refer to the "Configuring SIP MWI Features" section in the [SIP 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 conveys 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.

The SIP Voice Gateways feature is supported for analog endpoints that are connected to Foreign Exchange Station (FXS) ports or a Cisco VG224 Analog Phone Gateway and controlled by a Cisco call-control system, such as a Cisco Unified Communications Manager (Cisco Unified CM) or a Cisco Unified Communications Manager Express (Cisco Unified CME).

For more information on SIP Gateway features and information about configuring the SIP voice gateway for VoIPv6, see the [Configuring VoIP for IPv6](#).

---

**VoIPv6 Support on Cisco UBE**

Cisco UBE in VoIPv6 adds IPv6 capability to VoIP features. This feature adds dual-stack support on voice gateways, IPv6 support for SIP trunks, support for SCCP-controlled analog voice gateways, 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 [Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager](#)
- "SCCP-controlled analog voice gateways" section in the [SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways](#)
- "RTCP Pass-Through" section in [Cisco UBE RTCP Voice Pass-Through for IPv6](#)
- "T.38 fax over IPv6" section in [Fax, Modem, and Text Support over IP Configuration Guide](#)

Support has been added for audio calls in media Flow—Through (FT) and Flow—Around (FA) modes, High Density (HD) transcoding, 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 Cisco UBE.
Cisco UBE being a signaling proxy processes all signaling messages for setting up media channels. This enables Cisco UBE 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→EO
  - DO→DO
  - DO→EO

- Media Flow-Through (FT): In a media flow–through mode, between two endpoints, both signaling and media flows through the IP-to-IP Gateway (IPiP GW). The IPIP GW performs both signaling and media interworking between H.323/SIP IPv4 and SIP IPv6 networks.

Figure 15: H.323/SIP IPv4 – SIP IPv6 interworking in media flow-through mode

- Media Flow-Around (FA): Media flow–around provides the ability to have a SIP video call whereby signaling passes through Cisco UBE and media pass directly between endpoints bypassing the Cisco UBE.

Figure 16: H.323/SIP IPv4 - SIP IPv6 interworking in media flow-around mode

- Assisted RTCP (RTCP Keepalive): Assisted Real-time Transport Control Protocol (RTCP) enables Cisco UBE to generate RTCP keepalive reports on behalf of endpoints; however, endpoints, such as second generation Cisco IP phones (7940/7960) and Nortel Media Gateways (MG 1000T) do not generate any RTCP keepalive reports. Assisted RTCPs enable customers to use Cisco UBE to interoperate between endpoints and call control agents, such as Microsoft OCS/Lync so that RTCP reports are generated to indicate session liveliness during periods of prolonged silence, such as call hold or call on mute.
The assisted RTCP feature helps Cisco UBE 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 a call on hold or a call on mute.

• **SDP Pass-through**: SDP is configured to pass through transparently at the Cisco UBE, so that both the remote ends can negotiate media independently of the Cisco UBE.

SDP pass-through is addressed in two modes:

  • Flow-through—Cisco UBE plays no role in the media negotiation, it blindly terminates and re-originate the RTP packets irrespective of the content type negotiated by both the ends. This supports address hiding and NAT traversal.
  
  • Flow-around—Cisco UBE 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**: Cisco UBE 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 Cisco UBE are not detected because Cisco UBE 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 Cisco UBE. As Cisco UBE 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 "Cisco UBE 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 Cisco UBE 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 Cisco UBE 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-SIPConnections 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 Cisco UBE” 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 Cisco UBE 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. Cisco UBE monitors these endpoints periodically.

For more information, refer to the “Cisco UBE 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**: Cisco UBE 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 Cisco UBE interworks between different dynamic payload type values across the call legs for the same codec. Also, Cisco UBE 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 Cisco UBE 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, Cisco UBE inserts/removes/modifies the transcorder as needed.

Support for negotiation of an Audio Codec on each leg of a SIP–SIP call on the Cisco UBE feature supports negotiation of an audio codec using the Voice Class Codec (VCC) infrastructure on Cisco UBE. VCC supports SIP-SIP calls on Cisco UBE and allows mid-call codec change for supplementary services.
How to Configure VoIP for IPv6

Configuring VoIP for IPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints. 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.

A SIP trunk uses the Alternative Network Address Transport (ANAT) mechanism to exchange multiple IPv4 and IPv6 media addresses for the endpoints in a session. ANAT is automatically enabled on SIP trunks in dual-stack mode. The ANAT Session Description Protocol (SDP) grouping framework allows user agents (UAs) to include both IPv4 and IPv6 addresses in their SDP session descriptions. The UA is then able to use any of its media addresses to establish a media session with a remote UA.

A Cisco Unified Border Element can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco Unified Border Element, and the Cisco Unified Border Element performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 17: H.323/SIP IPv4--SIP IPv6 Interoperating in Media Flow-Through Mode

Shutting Down or Enabling VoIPv6 Service on Cisco Gateways

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. shutdown [ forced]
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>voice service voip</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# voice service voip</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Shuts down or enables VoIP call services.</td>
</tr>
<tr>
<td>shutdown [forced]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-voi-serv)# shutdown forced</td>
</tr>
</tbody>
</table>

### Shutting Down or Enabling VoIPv6 Submodes on Cisco Gateways

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. call service stop [forced]

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> call service stop [forced]</td>
<td>Shuts down or enables VoIPv6 for the selected submode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-serv-sip)# call service stop</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** sip-ua | Enters SIP user agent configuration mode. |
| **Step 4** protocol mode ipv4 | Configures the Cisco IOS SIP stack in dual-stack mode.  
ipv6 | dual-stack preference {ipv4 | ipv6}] |

### 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.

```plaintext
Device(config)# sip-ua  
Device(config-sip-ua)# protocol mode dual-stack preference ipv6
```

### Disabling ANAT Mode

ANAT is automatically enabled on SIP trunks in dual-stack mode. Perform this task to disable ANAT in order to use a single-stack mode.

### SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. no anat
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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 VoIP configuration mode. |
| **Step 4**
| sip
| Example:
Device(config-voi-serv)# sip |
| Enters SIP configuration mode. |
| **Step 5**
| no anat
| Example:
Device(conf-serv-sip)# no anat |
| Disables ANAT on a SIP trunk. |

### Verifying SIP Gateway Status

**Before You Begin**

To verify the status of SIP Gateway, use the following commands

### SUMMARY STEPS

1. show sip-ua calls
2. show sip-ua connections
3. show sip-ua status
DETAILED STEPS

Step 1  show sip-ua calls
The show sip-ua calls command displays active user agent client (UAC) and user agent server (UAS) information on SIP calls:

```
Device# show sip-ua calls
SIP UAC CALL INFO
Call 1
SIP Call ID : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
  State of the call     : STATE_ACTIVE (7)
  Substate of the call : SUBSTATE_NONE (0)
  Calling Number       : 2000
  Called Number        : 1000
  Bit Flags            : 0xC04018 0x100 0x0
  CC Call ID           : 2
  Source IP Address (Sig ) : 2001:DB8:0:ABCD::1
  Destn SIP Req Addr:Port : 2001:DB8:0:0:FFFF:5060
  Destn SIP Resp Addr:Port: 2001:DB8:0:1:FFFF:5060
  Destination Name     : 2001::21B:D5FF:FE1D:6C00
  Number of Media Streams : 1
  Number of Active Streams: 1
  RTP Fork Object      : 0x0
  Media Mode           : flow-through
  Media Stream 1
    State of the stream : STREAM_ACTIVE
    Stream Call ID      : 2
    Stream Type         : voice-only (0)
    Stream Media Addr Type : 1709707780
    Negotiated Codec   : (20 bytes)
    Codec Payload Type : 18
    Negotiated Dtmf-relay : inband-voice
    Dtmf-relay Payload Type : 0
    Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
    Media Dest IP Addr:Port : [2001::21B:D5FF:FE1D:6C00]:19548
  Options-Ping ENABLED:NO ACTIVE:NO
Number of SIP User Agent Client(UAC) calls: 1
```

Step 2  show sip-ua connections
Use the show sip-ua connections command to display SIP UA transport connection tables:

```
Example:
Device# show sip-ua connections udp brief
Total active connections : 1
No. of send failures      : 0
No. of remote closures    : 0
No. of conn. failures     : 0
No. of inactive conn. ageouts : 0
Router# show sip-ua connections udp detail
Total active connections : 1
No. of send failures      : 0
```
No. of remote closures : 0
No. of conn. failures : 0
No. of inactive conn. ageouts : 0

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

Remote-Agent:2001::21B:D5FF:FE1D:6C00, Connections-Count:1
Remote-Port Conn-Id Conn-State Write-Q-Size
========== ======= =========== ===========
      5060     2 Established          0

**Step 3**
show sip-ua status
Use the **show sip-ua status** command to display the status of the SIP UA:

**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): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED

**protocol mode is ipv6**
SDP application configuration:
Version line (v=) required
Owner line (o=) required
Timespec line (t=) required
Media supported: audio video image
Network types supported: IN
Address types supported: IP4 IP6
Transport types supported: RTP/AVP udptl

---

**RTCP Pass-Through**

IPv4 and IPv6 addresses embedded within RTCP packets (for example, RTCP CNAME) are passed on to Cisco UBE without being masked. These addresses are masked on the Cisco UBE ASR 1000.

The Cisco UBE ASR 1000 does not support printing of RTCP debugs.
RTCP is passed through by default. No configuration is required for RTCP pass-through.

**Configuring IPv6 Support for Cisco UBE**

In Cisco UBE, IPv4-only and IPv6-only modes are not supported when endpoints are dual-stack. In this case, Cisco UBE 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>sip-ua</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# sip-ua</td>
</tr>
<tr>
<td></td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>protocol mode {ipv4</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-sip-ua)# protocol mode ipv6</td>
</tr>
<tr>
<td></td>
<td>Configures the Cisco IOS SIP stack.</td>
</tr>
<tr>
<td></td>
<td>• protocol mode dual-stack preference {ipv4</td>
</tr>
<tr>
<td></td>
<td>• protocol mode {ipv4</td>
</tr>
</tbody>
</table>
|                   | • 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.
**Purpose**

Command or Action | Purpose
--- | ---
**Step 5** | **end** | Exits SIP user-agent configuration mode.
**Example:** | **Device**(conf-voi-serv)# **end**

---

### Verifying RTP Pass-Through

To enable RTCP packet-related debugging, use the following command:

**SUMMARY STEPS**

1. debug voip rtcp packets

**DETAILED STEPS**

```
debug voip rtcp packets
```

**Example:**

```
Device# debug voip rtcp packets

*Feb 14 06:24:58.799: //1/xxxxxxxxxxxx/RTP//Packet/voip_remote_rtcp_packet: Received RTCP packet
*Feb 14 06:24:58.799: SR: ssrc=0x1F7A35F0 sr_ntp_h=0xD10346B4 sr_ntp_l=0x13173DF8 sr_timestamp=0x0 sr_npackets=381 sr_nbytes=62176
*Feb 14 06:24:58.799: RR: ssrc=0x1A1752F0 rr_loss=0x0 rr_ehsr=5748 rr_jitter=0 rr_lsr=0x0 rr_dlsr=0x0
*Feb 14 06:24:58.799: SDES: ssrc=0x1F7A35F0 name=1 len=39 data=0.0.0@2001:DB8:C18:5:21B:D4FF:FED7:52F0
*Feb 14 06:24:58.799: SR: ssrc=0x0 sr_ntp_h=0xD10346B4 sr_ntp_l=0x13173DF8 sr_timestamp=0x0 sr_npackets=381 sr_nbytes=62176
*Feb 14 06:24:58.799: RR: ssrc=0x1A1752F0 rr_loss=0x0 rr_ehsr=5748 rr_jitter=0 rr_lsr=0x0 rr_dlsr=0x0
*Feb 14 06:24:58.799: SDES: ssrc=0x1F7A35F0 name=1 len=39 data=0.0.0@2001:DB8:C18:5:21B:D4FF:FED7:52F0
*Feb 14 06:24:58.919:...
```

---

### Configuring 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>voice service voip</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# voice service voip</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>sip</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-voi-serv)# sip</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>bind {control</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-serv-sip)# bind control source-interface FastEthernet 0/0</td>
</tr>
</tbody>
</table>
Configuring the SIP Server

SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. sip-server {dns: host-name | ipv4: ipv4-address | ipv6: [ipv6-address] :[port-nums]}
5. keepalive target {ipv4: address | ipv6: address | [port] | dns: hostname | tcp | udp | secondary}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>enable</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>sip-ua</td>
</tr>
<tr>
<td>Example:</td>
<td>sip-ua</td>
</tr>
<tr>
<td>Device(config)# sip-ua</td>
<td>Enters SIP user agent configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>sip-server {dns: host-name</td>
</tr>
</tbody>
</table>

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
### Purpose

**Command or Action**

**Purpose**

| Step 5 | keepalive target {ipv4 : address | ipv6 : address | : port | dns : hostname | tcp | tls | udp | secondary} | Identifies SIP servers that will receive keepalive packets from the SIP gateway. |
|---|---|---|
| Example: | Device(config-sip-ua)# keepalive target ipv6: 2001:DB8:0:0:8:800:200C:417A | |

### Example: Configuring the SIP Server

```
Device(config)# sip-ua
Device(config-sip-ua)# sip-server ipv6: 2001:DB8:0:0:8:800:200C:417A
```

## Configuring 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: SsS | SdS | SeS | SuS | host-name | enum:table-num | loopback:rtp | ras | sip-server | : port}

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters SIP user agent configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> registrar {dns: address</td>
<td>ipv4: destination-address [:port]</td>
</tr>
<tr>
<td>Example: Device(config-sip-ua)# registrar ipv6: 2001:DB8::20F:F7FF:FE0B:2972 expires 3600 secondary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> retry register retries</td>
<td>Configures the total number of SIP register messages that the gateway should send.</td>
</tr>
<tr>
<td>Example: Device(config-sip-ua)# retry register 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> timers register milliseconds</td>
<td>Configures how long the SIP UA waits before sending register requests.</td>
</tr>
<tr>
<td>Example: Device(config-sip-ua)# timers register 500</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Configuring SIP Register Support**

Device(config)# sip-ua
Device(config-sip-ua)# registrar ipv6: 2001:DB8::20F:F7FF:FE0B:2972 expires 3600 secondary
Device(config-sip-ua)# retry register 10
Device(config-sip-ua)# timers register 500
Configuring Outbound Proxy Server Globally on a SIP Gateway

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. outbound-proxy {ipv4: ipv4-address | ipv6: ipv6-address | dns: host : domain} [: port-number]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
|  | Example:  
Device> enable |  |
| Step 2 | configure terminal | Enters global configuration mode. |
|  | Example:  
Device# configure terminal |  |
| Step 3 | voice service voip | Enters voice service VoIP configuration mode. |
|  | Example:  
Device(config)# voice service voip |  |
| Step 4 | sip | Enters sip configuration mode. |
|  | Example:  
Device(config-voi-serv)# sip |  |
| Step 5 | outbound-proxy {ipv4: ipv4-address | ipv6: ipv6-address | dns: host : domain} [: port-number] | Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway using an IPv6 address. |
|  | Example:  
Device(config-serv-sip)# outbound-proxy ipv6: 2001:DB8::0:0:8:800:200C:417A |  |
Configuring UDP Checksum

SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 udp checksum [process | cef | none]
4. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
Example:  
Device> enable  
• Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
Example:  
Device# configure terminal |
| **Step 3** ipv6 udp checksum [process | cef | none] | Configures UDP checksum for Cisco UBE so that when you enable UDP checksum, it is computed and added for outgoing media packets. Similarly, disable the command to ignore the checksum calculation.  
Example:  
Device(config)# ipv6 udp checksum process  
Use the following keywords with the ipv6 udp checksum command:  
• process: Packets are punted to the process switching path for checksum validation.  
• cef: The UDP checksum validation is done in the CEF path.  
• none: UDP checksum validation is not done for received media packets in the CEF path and there is no UDP checksum computation for transmitted media packets. |
| **Step 4** exit | Exits global configuration mode and returns to privileged EXEC mode.  
Example:  
Device(config)# exit |
Configuring 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
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>voice service voip</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters IP address trusted list configuration mode. You can add unique</td>
</tr>
<tr>
<td>ip address trusted list</td>
<td>and multiple IP addresses for incoming VoIP (H.323/SIP) calls to a</td>
</tr>
<tr>
<td>Example:</td>
<td>list of trusted IP addresses.</td>
</tr>
<tr>
<td>Device(config-voi-serv)# ip address</td>
<td></td>
</tr>
<tr>
<td>trusted list</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enters IPv6 addresses for toll fraud prevention.</td>
</tr>
<tr>
<td>ipv6 X::X::X::X</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(cgf-iptrust-list)# ipv6 2001:</td>
<td></td>
</tr>
<tr>
<td>DB8::/48</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the RTP Port Range for an Interface

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `allow-connections sip to sip`
5. `media-address range range`
6. `rtp-port range range`
7. `exit`
8. `dial-peer voice tag voip`
9. `voice–class sip bind media source–interface interface`
10. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>voice service voip</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# voice service voip</code></td>
</tr>
</tbody>
</table>

Example:

Device(config-iptrust-list)# end

Exits trusted list configuration mode and returns to global configuration mode.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>allow-connections sip to sip</code></td>
<td>Allows sip-to-sip connections under voice service voip configuration mode for Cisco UBE.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(conf-voi-serv)# allow-connections sip to sip</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>media-address range range</code></td>
<td>Configures the media-address range, which enables the media gateway to allocate the available free port for a given IP address within the address range.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-voi-serv)# media-address range 2001:DB8::/48</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>rtp-port range range</code></td>
<td>Configures the RTP port range.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Each Cisco UBE can configure ten unique IP address ranges.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The default global RTP port range is from 16384 to 32766.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-voi-serv)# rtp-port range 20000 30000</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>exit</code></td>
<td>Exits voice service VoIP configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-voi-serv)# exit</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>dial-peer voice tag voip</code></td>
<td>Enters dial peer configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config)# dial-peer voice 300 voip</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>voice-class sip bind media source–interface interface</code></td>
<td>Matches the local SIP bind media IP address to the IP address range entries. Binds media packets to the IPv4 or IPv6 address of a specific interface and specifies an interface as the source address of SIP packets.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-dial-peer)# voice-class sip bind media source–interface GigabitEthernet 0</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>end</code></td>
<td>Exits dial peer configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-dial-peer)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Message Waiting Indicator Server Address

SUMMARY STEPS

1. **enable**
2. configure terminal
3. sip-ua
4. mwi-server {ipv4: destination-address | ipv6: destination-address | dns: host-name} peer-tag [output-dial-peer-tag]
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mwi-server {ipv4: destination-address</td>
<td>ipv6: destination-address</td>
</tr>
<tr>
<td>Example: Device(config-sip-ua)# mwi-server ipv6 2001:db8::/48 peer-tag 3</td>
<td>• ipv4/ ipv6: destination-address—IP address of the voice-mail server.</td>
</tr>
<tr>
<td></td>
<td>• dns: host-name—Host device housing the domain name server that resolves the name of the voice-mail server. The argument should contain the complete hostname to be associated with the target address; for example, dns:test.example.com.</td>
</tr>
<tr>
<td></td>
<td>• peer-tag—Attaches an existing dial peer to SIP MWI service.</td>
</tr>
</tbody>
</table>
### Configuring Voice Ports

#### SUMMARY STEPS

1. enable
2. configure terminal
3. voice-port port number
4. vmwi [fsk | dc-voltage]
5. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>voice-port port number</td>
<td>Enters voiceport configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# voice-port 3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>vmwi [fsk</td>
<td>dc-voltage]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-voiceport)# vmwi fsk</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action   | Purpose
---|---
| • If an FSK phone is connected to the voice port, use the `fsk` keyword. Similarly, if a DC voltage phone is connected to the voice port, use the `dc-voltage` keyword.

Step 5   end   Exits voice-port configuration mode and returns to privileged EXEC mode.

Example:

```
Device(config-voiceport)# end
```

---

Configuring Cisco UBE Mid-call Re-INVITE Consumption

Configuring 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 signalling changes only when bidirectional media is added.
   - `midcall-signaling passthru media-change` in Global VoIP SIP configuration mode.
   - `voice-class sip mid-call signaling passthru media-change` in dial-peer configuration mode.
4. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device&gt;</code> <code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**             |         |
| `configure terminal`   | Enters global configuration mode. |
| Example:               |         |
| `Device# configure terminal` | |
### Configuring Cisco UBE Mid-call Re-INVITE Consumption

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | Configure passthrough of mid-call signalling changes only when bidirectional media is added.  
- `midcall-signaling passthru media-change` in Global VoIP SIP configuration mode.  
- `voice-class sip mid-call signaling passthru media-change` in dial-peer configuration mode. | Re-Invites are passed through only when bidirectional media is added. |

**Example:**  
In Global VoIP SIP configuration mode:  
```
Device(config)# voice service voip  
Device(conf-voi-serv)# sip  
Device(conf-serv-sip)# midcall-signaling passthru media-change
```

**Example:**  
In Dial-peer configuration mode:  
```
Device(config)# dial-peer voice 2 voip  
Device(config-dial-peer)# voice-class sip mid-call signaling passthru media-change
```

| Step 4 | end | Exits to privileged EXEC mode. |

### Configuring Passthrough SIP Messages at Dial Peer Level

Perform this task to configure passthrough SIP messages at the dial-peer level. You need to perform this task at the dial-peer level to consume all media-related mid-call Re-INVITEs/UPDATES.

**Note**  
If the Cisco UBE Mid-call Re-INVITE/UPDATE consumption feature is configured on global and dial-peer level, dial-peer level takes precedence.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. `dial-peer voice dial-peer tag voip`  
4. `voice-class sip mid-call signaling passthru media-change`  
5. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters dial-peer voice configuration mode.</td>
</tr>
<tr>
<td>dial-peer voice <em>dial-peer tag voip</em></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Passes through SIP messages that involve media change.</td>
</tr>
<tr>
<td>voice-class sip mid-call signaling passthru media-change</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# voice-class sip mid-call signaling passthru media-change</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits dial-peer voice configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE

An organization with an IPv4 network can deploy a Cisco UBE on the boundary to connect with the service provider's IPv6 network (see the figure below).

**Figure 18: Cisco UBE Interoperating IPv4 Networks with IPv6 Service Provider**

A Cisco UBE can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco UBE, and the Cisco UBE performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

**Figure 19: IPv4 to IPv6 Media Interoperating Through Cisco IOS MTP**

The Cisco UBE feature adds IPv6 capability to existing VoIP features. This feature adds dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and SCCP-controlled analog voice gateways. In addition, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on an Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.
Before You Begin

Cisco UBE must be configured in IPv6-only or dual-stack mode to support IPv6 calls.

Note

A Cisco UBE interoperates between H.323/SIP IPv4 and SIP IPv6 networks only in media flow-through mode.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. allow-connections from type to to type

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> allow-connections from type to to type</td>
<td>Allows connections between specific types of endpoints in a VoIPv6 network.</td>
</tr>
<tr>
<td>Example: Device(config-voi-serv)# allow-connections h323 to sip</td>
<td>Arguments are as follows:</td>
</tr>
<tr>
<td></td>
<td>- from-type --Type of connection. Valid values: h323, sip.</td>
</tr>
<tr>
<td></td>
<td>- to-type --Type of connection. Valid values: h323, sip.</td>
</tr>
</tbody>
</table>
Example: Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE

```
Device(config)# voice service voip
Device(config-voi-serv)# allow-connections h323 to sip
```

Configuration Examples for VoIP over IPv6

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
```

Troubleshooting Tips for VoIP for IPv6

Media Flow-Through

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

To trace the execution path through the call control application programming interface (CCAPI), use the `debug voip ccap inout` command.

Media Flow-Around

To enable all Session Initiation Protocol (SIP)-related debugging, use the `debug ccsip all` command.

To trace the execution path through the call control application programming interface (CCAPI), use the `debug voip ccap inout` command.

SDP Pass-Through

To enable all Session Initiation Protocol (SIP)-related debugging (when the call is active in Pass through mode), use the `debug ccsip all` command.

RTP Port Range

To enable all Session Initiation Protocol (SIP)-related debugging, use the `debug ccsip all` command.

To enable debugging for Real-Time Transport Protocol (RTP) named event packets, use the `debug voip rtp` command.

VMWI SIP

To collect debug information only for signaling events, use the `debug vpm signal` command.

To show all Session Initiation Protocol (SIP) Service Provider Interface (SPI) message tracing, use the `debug ccsip messages` command.
Verifying and Troubleshooting Tips

Verifying Cisco UBE ANAT Call Flows

To verify that media settings are enabled in the media flowthrough and media flow-around feature, use the following commands:

**SUMMARY STEPS**

1. `show call active voice brief`
2. `show call active voice compact`
3. `show voip rtp connections`

**DETAILED STEPS**

**Step 1**  
`show call active voice brief`

**Example:**

```
Device> 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> 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>/0/0/0 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:<%
MODEMFAIL <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dli ci 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> xid:<rcvd>/sent total:<rcvd>/sent/drops
speeds(bps): local <rx/>ctx remote <rx/>tx
Proxy <ip>:<audio udps>,<video udps>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
x: <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
0 : 987 361904110ms.1 (16:01:10.557 IST Tue May 14 2013) +530 pid:1 Answer 1005 connected
dur 00:00:56 tx:1082/173120 rx:1141/182560 dscp:0 media:0 audio tos:0x88 video tos:0x0
IP 2001:1111:2222:3333:4444:5555:6666:1012:38356 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms
g711ulaw TextRelay: off Transcoded: No
media inactive detected media cntrl rcdn/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```
Verifying and Troubleshooting Cisco UBE ANAT Flow-Through Call

To verify and troubleshoot Cisco UBE ANAT Flow-Through calls, use the following commands:

**SUMMARY STEPS**

1. debug ccsip message
2. show voip rtp connections
**DETAILED STEPS**

**Step 1**

**debug ccsip message**

**Example:**

```
Device# show logging

*Jun 7 09:17:41.135: //1/xxxxxxxxxxx/SIP/Misc/ccsipDisplayMsg:
Received:
Date: Thu, 07 Jun 2012 10:47:17 GMT
Supported: 100rel,timer,resource-priority,recplaces
Require: sdp-anat
Min-SE: 1800
Cisco-Guid: 4231321369-294886243-2168545193-0797538600
User-Agent: Cisco-SIPGateway/IOS-12.x
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1339066037
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 441
v=0
a=SIP Call
c=IN IP4 9.44.30.10
a-group:ANAT 1 2
m=audio 16970 RTP/AVP 18 19
a=IN IP4 9.44.30.10
a-mid:1
a-rtpmap:18 G729/8000
a-fmt;p:18 annexb=no
a-rtpmap:19 CH/8000
a-ptime:20
m=audio 17066 RTP/AVP 18 19
a-mid:2
a-rtpmap:18 G729/8000
a-fmt;p:18 annexb=no
a-rtpmap:19 CH/8000
a-ptime:20

*Jun 7 09:17:41.159: //31/FC34D7198140/SIP/Misc/ccsipDisplayMsg:
Sent:
Date: Thu, 07 Jun 2012 10:47:17 GMT
Supported: 100rel,timer,resource-priority,recplaces
Require: sdp-anat
Min-SE: 1800
Cisco-Guid: 4231321369-294886243-2168545193-0797538600
User-Agent: Cisco-SIPGateway/IOS-12.x
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1339066037
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 441
v=0
a=SIP Call
```
Sent:
INVITE sip:6000@9.44.30.11:5060 SIP/2.0
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK2688E
Remote-Party-ID: <sip:1001@9.44.30.14>;party=calling;screen=no;privacy=off
From: <sip:1001@9.44.30.14>;tag=6D0FC0-1428
To: <sip:6000@9.44.30.11>
Date: Thu, 07 Jun 2012 09:17:41 GMT
Call-ID: 7780227E-ABFB811E-0800F3DD-5665AA1B@9.44.30.14
Supported: timer,resource-priority, replaces
Require: sdp-anat
Min-SE: 1800
Cisco-Guid: 4231321369-2948862433-2168455193-0797538600
User-Agent: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1339060661
Contact: <sip:1001@9.44.30.14:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Content-Type: application/sdp
Content-Disposition: session;handling=required Phone is offhook
Content-Length: 437
v=0
o=CiscoSystemsSIP-GW-UserAgent 3184 51 IN IP4 9.44.30.14
s=SIP Call
t=0 0
a=group:ANAT 1 2
m=audio 16438 RTP/AVP 18 19
a=mid:1
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000
a=ptime:20
m=audio 16440 RTP/AVP 18 19
c=IN IP4 9.44.30.14
a=mid:2
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000
a=ptime:20

*Jun 7 09:17:41.179: //32/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK2688E
From: <sip:1001@9.44.30.14>;tag=6D0FC0-1428
To: <sip:6000@9.44.30.11>
Date: Thu, 07 Jun 2012 10:40:14 GMT
Call-ID: 7780227E-ABFB811E-0800F3DD-5665AA1B@9.44.30.14
Timestamp: 1339060661
CSeq: 101 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Content-Length: 0

*Jun 7 09:17:41.203: //32/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK2688E
From: <sip:1001@9.44.30.14>;tag=6D0FC0-1428
To: <sip:6000@9.44.30.11>;tag=93D1F9D4-9E2
Date: Thu, 07 Jun 2012 10:40:14 GMT
Call-ID: 7780227E-ABFB811E-0800F3DD-5665AA1B@9.44.30.14
Timestamp: 1339060661
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@9.44.30.11>;party=called;screen=no;privacy=off
Contact: <sip:6000@9.44.30.11:5060>
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Content-Length: 0

*Jun 7 09:17:41.207: //31/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
  Sent:
  SIP/2.0 180 Ringing
Via: SIP/2.0/UDP [2001:DB8:C18:2:219:2FFF:FE89:7928]:5060;branch=z9hG4bK1CA8CD
Date: Thu, 07 Jun 2012 09:17:41 GMT
Timestamp: 1339066037
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.2.20120528.102328.
Content-Length: 0

*Jun 7 09:17:41.219: //32/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
  Received:
  SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK2688E
From: <sip:1001@9.44.30.14>;tag=6D0FC0-1428
To: <sip:6000@9.44.30.11>;tag=93D1F9D4-9E2
Date: Thu, 07 Jun 2012 10:40:14 GMT
Call-ID: 7780227E-AFB811E1-8060F4DD-5665AA1B@9.44.30.14
Timestamp: 1339060661
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@9.44.30.11>;party=called;screen=no;privacy=off
Contact: <sip:6000@9.44.30.11:5060>
Supported: replaces
Require: sip-anat
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 435
v=0
o=CiscoSystemsSIP-GW-UserAgent 8213 2783 IN IP4 9.44.30.11
s=SIP Call
c=IN IP6 2001:DB8:C18:2:217:59FF:FEDE:8898
t=0 0
a=group:ANAT 1
m=audio 17200 RTP/AVP 18 19
c=IN IP6 2001:DB8:C18:2:217:59FF:FEDE:8898
a-mid:1
a=rtpmap:18 G729/8000
a=fmttype:18 annexb=no
a=rtpmap:19 CN/8000
a-ptime:20
m=audio 0 RTP/AVP 18 19
c=IN IP4 9.44.30.11
a-mid:2
a=rtpmap:18 G729/8000
a=fmttype:18 annexb=no
a=rtpmap:19 CN/8000
a-ptime:20

*Jun 7 09:17:41.227: //32/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
  Sent:
  ACK sip:6000@9.44.30.11:5060 SIP/2.0
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK27145B
Verifying and Troubleshooting Cisco UBE ANAT Flow-Through Call

From: <sip:1001@9.44.30.14>;tag=6D0FC0-1428
To: <sip:6000@9.44.30.11>;tag=93D1F9D4-9E2
Date: Thu, 07 Jun 2012 09:17:41 GMT
Call-ID: 7760227E-AB8811E1-0060F4DD-5665AA89@9.44.30.14
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

*Jun 7 09:17:41.235: //31/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:DB8:C18:2:219:2FF:FE89:7928];branch=z9hG4bK1CA8CD
From: <sip:1001@2001:DB8:C18:2:219:2FF:FE89:7928>;tag=6EDAC1D0-F25
To: <sip:6000@2001:DB8:C18:2:223:4FF:FEAC:4540>;tag=600FF4-14D3
Date: Thu, 07 Jun 2012 09:17:41 GMT
Timestamp: 1339066037
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@2001:DB8:C18:2:223:4FF:FEAC:4540>;party=called;screen=no;privacy=off
Contact: <sip:6000@2001:DB8:C18:2:223:4FF:FEAC:4540>;tag=5060
Supported: replaces
Require: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 433
v=0
s=SIP Call
c=IN IP4 9.44.30.14
t=0 0
a=group:ANAT 1
m=audio 16436 RTP/AVP 18 19
c=IN IP4 9.44.30.14
a=midi1
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000
a=ptime:20
m=audio 0 RTP/AVP 18 19
m=audio 0 RTP/AVP 18 19
a=midi2
a=rtpmap:18 G729/8000
a=rtpmap:18 annexb-no
a=rtpmap:19 CN/8000
a=ptime:20

*Jun 7 09:17:41.251: //31/FC34D7198140/SIP/Msg/ccsipDisplayMsg:
Received:
ACK sip:60008@2001:DB8:C18:2:223:4FF:FEAC:4540];tag=5060 SIP/2.0
Via: SIP/2.0/UDP [2001:DB8:C18:2:219:2FF:FE89:7928];branch=z9hG4bK1CB1E77
From: <sip:1001@2001:DB8:C18:2:219:2FF:FE89:7928];tag=6EDAC1D0-F25
To: <sip:6000@2001:DB8:C18:2:223:4FF:FEAC:4540];tag=600FF4-14D3
Date: Thu, 07 Jun 2012 10:47:17 GMT
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

Step 2 show voip rtp connections
### Example:

Device# **show voip rtp connections**

**VoIP RTP Port Usage Information:**
Max Ports Available: 8091, Ports Reserved: 101, Ports in Use: 3
Port range not configured, Min: 16384, Max: 32767

<table>
<thead>
<tr>
<th>Media-Address Range</th>
<th>Ports Available</th>
<th>Ports Reserved</th>
<th>Ports In-use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Address-Range</td>
<td>8091</td>
<td>101</td>
<td>3</td>
</tr>
</tbody>
</table>

**VoIP RTP active connections:**

<table>
<thead>
<tr>
<th>No.</th>
<th>CallId</th>
<th>dstCallId</th>
<th>LocalRTP</th>
<th>RmtRTP</th>
<th>LocalIP</th>
<th>RemoteIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>31</td>
<td>32</td>
<td>16436</td>
<td>16970</td>
<td>9.44.30.14</td>
<td>9.44.30.10</td>
</tr>
</tbody>
</table>

Found 2 active RTP connections

---

**Verifying Cisco UBE ANAT Flow-Around Calls**

To verify Cisco UBE ANAT Flow-Around calls, use the **debug ccsip message** commands:

**SUMMARY STEPS**

1. **debug ccsip message**
2. **show voip rtp connections**

**DETAILED STEPS**

**Step 1  **debug ccsip message

**Example:**

Device# **show logging**

```
*Jun 7 17:26:30.681: //UserService::SIP/Msg/ccsipDisplayMsg: Received:
 Date: Thu, 07 Jun 2012 17:35:05 GMT
 Call-ID: F44F5437-AFFD11E1-616CD9DB-F669087E@2001:DB8:C18:2:223:33FF:FEB1:B440
 Supported: 100rel, timer, resource-priority, replaces
 Require: sdp-anat
 Min-SE: 1800
 Cisco-Guid: 1170397766-2953384417-2170945561-0797538600
 User-Agent: Cisco-SIPGateway/IOS-12.x
 Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
 CSeq: 101 INVITE
 Max-Forwards: 70
```
Verifying Cisco UBE ANAT Flow-Around Calls

Timestamp: 1339090505
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 465

v=0
s=SIP Call
c=IN IP4 9.44.30.13
t=0 0
a=group:ANAT 1 2
m=audio 18706 RTP/AVP 18 0 19
c=IN IP4 9.44.30.13
a=mid:1
a=rtmap:18 G729/8000
a=fmt:18 annexb=no
a=rtmap:0 PCMU/8000
a=rtmap:19 CN/8000
m=audio 16384 RTP/AVP 18 0 19
a=mid:2
a=rtmap:18 G729/8000
a=fmt:18 annexb=no
a=rtmap:0 PCMU/8000
a=rtmap:19 CN/8000

*Jun 7 17:26:30.705: //106/45C2DA46B166/SIP/Mgs/ccsipDisplayMsg:
Sent:
SIP/2.0 100 Trying
Date: Thu, 07 Jun 2012 17:26:30 GMT
Timestamp: 1339090505
CSeq: 101 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Content-Length: 0

*Jun 7 17:26:30.705: //107/45C2DA46B166/SIP/Mgs/ccsipDisplayMsg:
Sent:
INVITE sip:6000@9.44.30.11:5060 SIP/2.0
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK90BB
Remote-Party-ID: <sip:1001@9.44.30.14>;party=calling;screen=no;privacy=off
From: <sip:1001@9.44.30.14>;tag=22C984C-970
To: <sip:6000@9.44.30.11>
Date: Thu, 07 Jun 2012 17:26:30 GMT
Call-ID: C145AF07-AFFC11E1-813EF4DD-5665AA1B@9.44.30.11
Supported: timer,resource-priority,requires
Require: sdp-anat
Min-SE: 1800
Cisco-Guid: 1170397766-2953384417-2170945561-0797538600
User-Agent: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1339090505
Contact: <sip:1001@9.44.30.11:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 418
v=0
VoIP for IPv6

Verifying Cisco UBE ANAT Flow-Around Calls

IOS XE Release 3S

o=CiscoSystemsSIP-GW-UserAgent 9582 2407 IN IP4 9.44.30.14
c=SIP Call
t=0 0
m=audio 18706 RTP/AVP 18 19
c=IN IP4 9.44.30.13
m=audio 16384 RTP/AVP 18 19
c=IN IP6 2001:DB8:C18:2:223:33FF:FEB1:B440
*Jun 7 17:26:30.729: //107/45C2DA468166/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK90BB
From: <sip:1001@9.44.30.14>;tag=22C984C-970
To: <sip:6000@9.44.30.11>
Date: Thu, 07 Jun 2012 18:49:04 GMT
Call-ID: C145AF07-ACFC11E1-813E4DD-5665AA1B89.44.30.14
Timestamp: 1339089990
CSeq: 101 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Content-Length: 0

*Jun 7 17:26:30.753: //107/45C2DA468166/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=z9hG4bK90BB
From: <sip:1001@9.44.30.14>;tag=22C984C-970
To: <sip:6000@9.44.30.11>
Date: Thu, 07 Jun 2012 18:49:04 GMT
Call-ID: C145AF07-ACFC11E1-813E4DD-5665AA1B89.44.30.14
Timestamp: 1339089990
CSeq: 101 INVITE
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@9.44.30.11>;party=called;screen=no;privacy=off
Contact: <sip:6000@9.44.30.11:5060>
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Content-Length: 0

*Jun 7 17:26:30.753: //107/45C2DA468166/SIP/Msg/ccsipDisplayMsg:
Sent:
SIP/2.0 180 Ringing
From: <sip:1001@2001:DB8:C18:2:223:33FF:FEB1:B440>;tag=5569EC8-C79
To: <sip:6000@2001:DB8:C18:2:223:33FF:FEB1:B440>;tag=22C9880-150D
Date: Thu, 07 Jun 2012 17:26:30 GMT
Timestamp: 1339090505
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@2001:DB8:C18:2:223:33FF:FEB1:B440>;party=called;screen=no;privacy=off
Contact: <sip:6000@2001:DB8:C18:2:223:33FF:FEB1:B440>;tag=22C9880-150D
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Content-Length: 0
**Verifying Cisco UBE ANAT Flow-Around Calls**

*Jun 7 17:26:30.765: //107/45C2DA468166/SIP/Msg/ccsipDisplayMsg:*

```
Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.44.30.14;branch=zd9hG4Bk90BB
From: <sip:6000@9.44.30.14>;tag=959183D0-2073
To: <sip:6000@9.44.30.11>;tag=959183D0-2073
Date: Thu, 07 Jun 2012 18:49:04 GMT
Call-ID: C145AF07-AFFC11E1-813EF4DD-5665AA1B@9.44.30.14
Timestamp: 1339099990
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@9.44.30.11>;party=called;screen=no;privacy=off
Contact: <sip:6000@9.44.30.11:5060>
Supported: replaces
Require: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 412

v=0
o=CiscoSystemsSIP-GW-UserAgent 2764 5975 IN IP4 9.44.30.11
s=SIP Call
c=IN IP4 9.44.30.11
t=0 0
a=group:ANAT 1
m=audio 17278 RTP/AVP 18 19
  c=IN IP4 9.44.30.11
  a=mid:1
  a=rtpmap:18 G729/8000
  a=fmtp:18 annexb=no
  a=rtpmap:19 CN/8000
  a=ptime:20
m=audio 0 RTP/AVP 18 19
  c=IN IP6 2001:DB8:C18:2:223:33FF:FEB1:B440
  a=mid:2
  a=rtpmap:18 G729/8000
  a=fmtp:18 annexb=no
  a=rtpmap:19 CN/8000
  a=ptime:20
```

*Jun 7 17:26:30.777: //107/45C2DA468166/SIP/Msg/ccsipDisplayMsg:*

```
Sent:
ACK sip:6000@9.44.30.11:5060 SIP/2.0
Via: SIP/2.0/UDP 9.44.30.14:5060;branch=zd9hG4Bk91207D
From: <sip:6000@9.44.30.14>;tag=959183D0-2073
To: <sip:6000@9.44.30.11>;tag=959183D0-2073
Date: Thu, 07 Jun 2012 17:26:30 GMT
Call-ID: C145AF07-AFFC11E1-813EF4DD-5665AA1B@9.44.30.14
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0
```

*Jun 7 17:26:30.785: //106/45C2DA468166/SIP/Msg/ccsipDisplayMsg:*

```
Sent:
SIP/2.0 200 OK
From: <sip:6000@2001:DB8:C18:2:223:33FF:FE85:B440>;tag=5569ECC8-C79
To: <sip:6000@2001:DB8:C18:2:223:33FF:FE85:B440>;tag=5569ECC8-C79
Date: Thu, 07 Jun 2012 17:26:30 GMT
Timestamp: 1339090505
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:6000@2001:DB8:C18:2:223:33FF:FE85:B440>;party=called;screen=no;privacy=off
```
Supported: replaces
Require: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 421

v=0
s=SIP Call
c=IN IP4 9.44.30.11
t=0 0
a=group:ANAT 1
m=audio 17278 RTP/AVP 18 19
c=IN IP4 9.44.30.11
a=mid:1
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000
a=ptime:20
m=audio 0 RTP/AVP 18 19
c=IN IP6 2001:DB8:C18:2:217:59FF:FEDE:8898
a=mid:2
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:19 CN/8000

*Jun 7 17:26:30.793: /-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
Date: Thu, 07 Jun 2012 17:35:05 GMT
Call-ID: F44F5437-AFFD11E1-816CD9DB-F669887E@2001:DB8:C18:2:223:33FF:FEDE:8898
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

Step 2

```
show voip rtp connections  
```

Example:

```
Device# show voip rtp connections

VoIP RTP Port Usage Information:
Max Ports Available: 8091, Ports Reserved: 101, Ports in Use: 0
Port range not configured, Min: 16384, Max: 32767

<table>
<thead>
<tr>
<th>Media-Address Range</th>
<th>Ports Available</th>
<th>Ports Reserved</th>
<th>Ports In-use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Address-Range</td>
<td>8091</td>
<td>101</td>
<td>0</td>
</tr>
</tbody>
</table>

No active connections found
```
Verifying VMWI SIP

SUMMARY STEPS

1. show sip-ua mwi
2. debug vpm signal
3. debug ccsip messages

DETAILED STEPS

Step 1  show sip-ua mwi

Example:
Device# show sip-ua mwi
MWI type: 2
MWI server: 2001:10:12:1::2006  //IPv6 MWI Server Address//
MWI expires: 3600
MWI port: 5060
MWI dial peer tag: 0  //Shows the MWI-Server binding dial-peer tag. Tag "0" is default.//
MWI solicited  //MWI type is solicited by default. Subscription of voice-port is required in this case only.//
MWI ipaddr cnt 1:
MWI ipaddr idx 0:
MWI server: 2001:10:12:1::2006, port 5060, transport 1  //IPv6 MWI Server Address//
MWI server dns lookup retry cnt: 0

Step 2  debug vpm signal

Example:
Device# debug vpm signal
Process vmwi. vmwi state: OFF
The phone is not on hook (1). Delay the vmwi processing.  //Phone is offhook//
Process dc-voltage vmwi. State: OFF  //VMWI state is off//
*Mar 2 02:33:34.841: [2/0] c2400_dc_volt_mwi: on=0
The phone is not onhook (1). Delay the vmwi processing. Process vmwi. vmwi state: ON  //VMWI state is on//
Voice port 0/2/1 subscribed MWI  //Subscription of port for MWI (Solicited)//

Step 3  debug ccsip messages

Example:
Device# debug ccsip messages

Note  The debug ccsip messages command shows the SIP Messages, such as Subscribe and Notify.
Verifying SDP Passthrough Configuration

SUMMARY STEPS

1. debug csip all
2. show voip rtp connection

DETAILED STEPS

Step 1  debug csip all

Example:

```
Device# show logging

Received:
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:33FF:FE81:B440]:5060;branch=z9hG4bK20277F
Route: <sip:1001@[2001:DB8:C18:2:223:33FF:FE81:B440];party=calling;screen=no;privacy=off>
Date: Fri, 08 Jun 2012 11:01:48 GMT
Call-ID: 2D6EEC84-B09011F1-6233D98F-669887E82001:DB8:C18:2:223:33FF:FE81:B440
Supported: 100rel,timer,resource-priority,replaces
Require: sdp-anat
Min-SE: 1800
Cisco-Guid: 2131649325-2962952673-2175336473-0797538600
User-Agent: Cisco-SIPGateway/IOS-12.x
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1339153308
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 488
v=0
s=SIP Call
t=0 0
a=group:ANAT 1 2
m=audio 16406 RTP/AVP 18 0 19
a=rtmp=map:18 G729/8000
a=fmt=map:18 annexb=no
a=rtmp=map:0 PCMU/8000
a=rtmp=map:19 CN/8000
m=audio 18024 RTP/AVP 18 0 19
c=IN IP4 9.44.30.13
a=mid:2
a=rtmp=map:18 G729/8000
a=fmt=map:18 annexb=no
a=rtmp=map:0 PCMU/8000
a=rtmp=map:19 CN/8000

Sent:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:33FF:FE81:B440]:5060;branch=z9hG4bK20277F
```
Verifying SDP Passthrough Configuration

Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: 2D6EEC84-B09011E1-8235D9DB-F669887E@2001:DB8:C18:2:223:33FF:FEDE:8898
CSeq: 101 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Content-Length: 0

Sent:
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:4FF:FEDE:8898]:5060;branch=z9hG4bK15D1013
Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: FB05CC74-B08E11E1-82C1F4DD-5665AA18@2001:DB8:C18:2:223:4FF:FEDE:8898
Supported: timer,resource-priority,replaces,sdp-anat
Min-SE: 1800
Cisco-Guid: 2131649325-2962952673-2175336473-0797538600
User-Agent: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1339152794
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 60
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 443

v=0
s=SIP Call
t=0 0
a=group:ANAT 1 2
m=audio 16712 RTP/AVP 18 0 19
a=mid:1
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
m=audio 16714 RTP/AVP 18 0 19
c=IN IP4 9.44.30.14
a=mid:2
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000

*Jun 8 10:53:14.137: //243/7F0E632D81A9/SIP/Msg/ccsipDisplayMsg:
Received:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:4FF:FEAC:4540]:5060;branch=z9hG4bK15D1013
Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: FB05CC74-B08E11E1-82C1F4DD-5665AA18@2001:DB8:C18:2:223:4FF:FEDE:8898
CSeq: 101 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Content-Length: 0
Received:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:4FF:FEAC:4540]:5060;branch=z9hG4bK15D1013
VoIP for IPv6

Verifying SDP Passthrough Configuration

Date: Fri, 08 Jun 2012 12:15:49 GMT
Call-ID: FB05CC74-B08E11B1-82C1F4DD-5655A1B0@2001:DB8:C18:2:223:4FF:FEAC:4540
Timestamp: 1339152794
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Content-Length: 0

Sent:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:33FF:FEB1:B440]:5060;branch=z9hG4bK20277F
Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: 2D6EEC84-B09011E1-8235D9DB-F669887E@2001:DB8:C18:2:223:33FF:FEB1:B440
Timestamp: 1339153308
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.2.3.20120528.102328.
Content-Length: 0

Received:
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:33FF:FEB1:B440]:5060;branch=z9hG4bK15D1013
Date: Fri, 08 Jun 2012 12:15:49 GMT
Call-ID: FB05CC74-B08E11B1-82C1F4DD-5655A1B0@2001:DB8:C18:2:223:4FF:FEAC:4540
Timestamp: 1339152794
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Supported: replaces
Require: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.5.T
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 434

v=0
s=SIP Call
c=IN IP6 2001:DB8:C18:2:217:59FF:FEDE:8898
m=audio 17424 RTP/AVP 18 19
a=group:ANAT 1
a=mid:2
a=rtpmap:18 G729/8000
a=rtpmap:19 CN/8000
a=audio 0 RTP/AVP 18 19
c=IN IP4 9.44.30.11
a=mid:2
a=rtpmap:18 G729/8000
a=rtpmap:19 CN/8000

Sent:
Verifying SDP Passthrough Configuration

Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: FB05CC74-B08E11E1-02C1F4DD-5665AA18@2001:DB8:C18:2:223:4FF:FEAC:4540
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

Sent:
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:33FF:FEBC:B440]:5060;branch=z9hG4bK20277F
Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: 2D6EEC84-B09011E1-8235D9DB-F669887E@2001:DB8:C18:2:223:33FF:FEBC:B440
Timestamp: 1339153308
CSeq: 101 INVITE
Allow-Events: telephone-event
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.20120528.102328.
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 389

v=0
m=audio 16710 RTP/AVP 18 19
a=group:ANAT 1
m=audio 0 RTP/AVP 18 19
a=group:ANAT 2

Received:
Via: SIP/2.0/UDP [2001:DB8:C18:2:223:33FF:FEBC:B440]:5060;branch=z9hG4bK203700
Date: Fri, 08 Jun 2012 10:53:14 GMT
Call-ID: 2D6EEC84-B09011E1-8235D9DB-F669887E@2001:DB8:C18:2:223:33FF:FEBC:B440
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: telephone-event
Content-Length: 0

**Step 2**
show voip RTP connection

**Example:**
Device# show voip RTP connection

VoIP RTP Port Usage Information:
Max Ports Available: 8091, Ports Reserved: 101, Ports in Use: 2
Port range not configured, Min: 16384, Max: 32767
### Feature Information for VoIP for IPv6

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Media-Address Range</th>
<th>Available</th>
<th>Reserved</th>
<th>In-use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Address-Range</td>
<td>8091</td>
<td>101</td>
<td>2</td>
</tr>
</tbody>
</table>

VoIP RTP active connections:

<table>
<thead>
<tr>
<th>No.</th>
<th>CallId</th>
<th>dstCallId</th>
<th>LocalRTP</th>
<th>RmtRTP</th>
<th>LocalIP</th>
<th>RemoteIP</th>
</tr>
</thead>
</table>

Found 2 active RTP connections
### Table 27: Feature Information for VoIP for IPv6

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UBE support for IPv6</td>
<td>12.4(22)T</td>
<td>Cisco Unified Border Element (Cisco UBE) support for SIP IPv4-IPv6 dual stack and IPv4 and IPv6 capability provides the following functionality:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Translation of SIP IPv4 to IPv6 addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administration and enforcement of policies for the IPv4/IPv6 mode of operation of each component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supports the following scenarios: H.323 IPv4 to SIP IPv6; SIP IPv4 to SIP IPv6, SIP IPv6 to SIP IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DTMF: Interworking capability on Cisco UBE (H.245 Signal, RFC 2833, SIP Notify, Key Press Markup Language, H.323 to SIP, RFC 2833 to G.711 Inband)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPv6 topology hiding and demarcation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Options-ping</td>
</tr>
</tbody>
</table>

The VoIP for IPv6 feature describes the Session Border Controller (SBC) functionality of connecting a SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network that is implemented on a Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UBE support for IPv6</td>
<td>15.3(2)T</td>
<td></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following features are supported on Cisco UBE for 15.3(2)T:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assisted RTCP (RTCP Keepalive)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Audio Transcoding using Local Transcoding Interface (LTI)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Address Hiding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Call Transfer (re-INVITE, REFER)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Call Forward (302 based)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP Toll Fraud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hold/Resume</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Flow-Through (FT)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Flow-Around (FA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RE-INVITE Consumption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RTP Port Range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SDP Pass-Through</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UDP Checksum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Media Anti-Trombone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Header Passing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Refer-To Passing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Error Pass-through</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP UPDATE Interworking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Session timer (RFC 4028)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP OPTIONS Ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configurable Error Response Code in OPTIONS Ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limiting the Rate of Incoming SIP Calls per Dial-Peer (aka Call Spike)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Profiles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Media Inactivity Detection</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DSCP-Based QoS Support</td>
<td>12.4(22)T</td>
<td>IPv6 supports this feature.</td>
</tr>
<tr>
<td>IPv6 Dual Stack</td>
<td>12.4(22)T</td>
<td>Adds IPv6 capability to existing VoIP features on the Cisco UBE. Additionally, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to SIP IPv6 network is implemented on a Cisco UBE to facilitate migration from VoIPv4 to VoIPv6. The following commands were introduced or modified: None</td>
</tr>
<tr>
<td>RTP/RTCP over IPv6</td>
<td>12.4(22)T</td>
<td>RTP stack supports the ability to create IPv6 connections using IPv6 unicast and multicast addresses as well as IPV4 connections.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TDM-SIP GW for IPv6</td>
<td>12.4(24)T</td>
<td>IPv6 supports this feature.</td>
</tr>
<tr>
<td></td>
<td>15.3(2)T</td>
<td>• Session Initiation Protocol Features Supported on IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco UBE features Supported on IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Gateway Generic Features</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Apart from the SIP Gateway features already supported on IPv4 and IPv6 for 12.4(24)T release, the following features are also supported on IPv6:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP VMWI for FXS phones</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• History-Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Handling 181/183 Responses with/without SDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Session Timer (4028)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIP Media Inactivity Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PPI/PAI &amp; Privacy (RFC3323/RFC3325) Headers</td>
</tr>
</tbody>
</table>

**VoIP for IPv6**

**Feature Information for VoIP for IPv6**

---


312
Interworking of Secure RTP calls for SIP and H.323

The Session Initiation Protocol (SIP) support for the Secure Real-time Transport Protocol (SRTP) is an extension of the Real-time Transport Protocol (RTP) Audio/Video Profile (AVP) and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets that provide authentication, encryption, and the integrity of media packets between SIP endpoints.

SIP support for SRTP was introduced in Cisco IOS Release 12.4(15)T. In this and later releases, you can configure the handling of secure RTP calls on both a global level and on an individual dial peer basis on Cisco IOS voice gateways. You can also configure the gateway (or dial peer) either to fall back to (nonsecure) RTP or to reject (fail) the call for cases where an endpoint does not support SRTP.

The option to allow negotiation between SRTP and RTP endpoints was added for Cisco IOS Release 12.4(20)T and later releases, as was interoperability of SIP support for SRTP on Cisco IOS voice gateways with Cisco Unified Communications Manager. In Cisco IOS Release 12.4(22)T and later releases, you can also configure SIP support for SRTP on Cisco Unified Border Elements (Cisco UBEs).

- Finding Feature Information, page 313
- Prerequisites for Interworking of Secure RTP calls for SIP and H.323, page 314
- Restrictions for Interworking of Secure RTP calls for SIP and H.323, page 314
- Feature Information for Configuring Interworking of Secure RTP Calls for SIP and H.323, page 315

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for Interworking of Secure RTP calls for SIP and H.323

The following are prerequisites for the Interworking of Secure RTP calls for SIP and H.323 feature:

- Establish a working IP network and configure VoIP.

Note

For information about configuring VoIP, see Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms at the following URL:

- Ensure that the gateway has voice functionality configured for SIP.
- Ensure that your Cisco router has adequate memory.
- As necessary, configure the router to use Greenwich Mean Time (GMT). SIP requires that all times be sent in GMT. SIP INVITE messages are sent in GMT. However, the default for routers is to use Coordinated Universal Time (UTC). To configure the router to use GMT, issue the clock timezone command in global configuration mode and specify GMT.

Cisco Unified Border Element

- Cisco IOS Release 12.2(20)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

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

Restrictions for Interworking of Secure RTP calls for SIP and H.323

- The SIP gateway does not support codecs other than those listed in the table titled "SIP Codec Support by Platform and Cisco IOS Release" in the "Enhanced Codec Support for SIP Using Dynamic Payloads" section of the Configuring SIP QoS Features module at the following URL:
- SIP requires that all times be sent in GMT.
Feature Information for Configuring Interworking of Secure RTP Calls for SIP and H.323

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interworking of Secure RTP calls for SIP and H.323</td>
<td>12.4(20)T</td>
<td>This feature provides an option for a Secure RTP (SRTP) call to be connected from H.323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands.</td>
</tr>
<tr>
<td>Interworking of Secure RTP calls for SIP and H.323</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>This feature provides an option for a Secure RTP (SRTP) call to be connected from H.323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands.</td>
</tr>
</tbody>
</table>
Cisco UBE Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows secure enterprise-to-enterprise 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)-Real-Time Transport Protocol (RTP) internetworking between one or multiple Cisco Unified Border Elements (Cisco UBEs) is enabled for SIP-SIP audio calls.

In Cisco IOS Release 15.2(1) and Cisco IOS XE Release 3.7S, the SRTP-RTP Interworking feature was extended to support supplementary services on Cisco UBEs.

- Prerequisites for CUBE Support for SRTP-RTP Internetworking, page 317
- Restrictions for CUBE Support for SRTP-RTP Internetworking, page 318
- Information About CUBE for SRTP-RTP Internetworking, page 318
- How to Configure Cisco UBE Support for SRTP-RTP Internetworking, page 321
- Configuration Examples for CUBE Support for SRTP-RTP Internetworking, page 339
- Feature Information for CUBE Support for SRTP-RTP Internetworking, page 341

Prerequisites for CUBE Support for SRTP-RTP Internetworking

- The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is supported in Cisco Unified CallManager 7.0 and later releases.

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)YB or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.7S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Restrictions for CUBE Support for SRTP-RTP Internetworking

The following features are not supported by the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature:

- Asymmetric SRTP fallback configurations
- Call admission control (CAC) support
- Rotary SIP-SIP
- SRTCP-RTCP interworking
- Transcoding for SRTP-SRTP audio calls

Note: Effective from Cisco IOS XE release 3.9S, SRTP-RTP interworking is supported (on ASR platforms) for video calls with no secondary video streams.

Information About CUBE for SRTP-RTP Internetworking

To configure support for SRTP-RTP internetworking, you should understand the following concepts:

CUBE Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP Cisco Unified CallManager domains with the following:

- RTP Cisco Unified CallManager domains. Domains that do not support SRTP or have not been configured for SRTP, as shown in the figure below.

- RTP Cisco applications or servers. For example, Cisco Unified MeetingPlace, Cisco WebEx, or Cisco Unity, which do not support SRTP, or have not been configured for SRTP, or are resident in a secure data center, as shown in the figure below.
• RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.

**Figure 20: SRTP Domain Connections**

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP internetworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible secure business-to-business communications without the need for static IPsec tunnels or the need to deploy SRTP within the enterprise, as shown in the figure below.

**Figure 21: Secure Business-to-Business Communications**
SRTP-RTP internetworking also connects SRTP enterprise networks with static IPSec over external networks, as shown in the figure below.

*Figure 22: SRTP Enterprise Network Connections*

SRTP-RTP internetworking on the Cisco UBE in a network topology uses single-pair key generation. Existing audio and dual-tone multifrequency (DTMF) transcoding is used to support voice calls. SRTP-RTP internetworking support is provided in both flow-through and high-density mode. SRTP-SRTP pass-through is not impacted.

SRTP is configured on one dial peer and RTP is configured on the other dial peer using the `srtp` and `srtp fallback` commands. The dial-peer configuration takes precedence over the global configuration on the Cisco UBE.

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. RTP-RTP fallback occurs when no transcoding resources are available for SRTP-RTP internetworking.

**TLS on the Cisco Unified Border Element**

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows Transport Layer Security (TLS) to be enabled or disabled between the Skinny Call Control Protocol (SCCP) server and the SCCP client. By default, TLS is enabled, which provides added protection at the transport level and ensures that SRTP keys are not easily accessible. Once TLS is disabled, the SRTP keys are not protected.

SRTP-RTP internetworking is available with normal and universal transcoders. The transcoder on the Cisco Unified Border Element is invoked using SCCP messaging between the SCCP server and the SCCP client. SCCP messages carry the SRTP keys to the digital signal processor (DSP) farm at the SCCP client. The transcoder can be within the same router or can be located in a separate router. TLS should be disabled only when the transcoder is located in the same router. To disable TLS, configure the `no` form of the `tls` command in dsp farm profile configuration mode. Disabling TLS improves CPU performance.

**Supplementary Services Support on the Cisco UBE for RTP-SRTP Calls**

The Supplementary Services Support on Cisco UBE for RTP-SRTP Calls feature supports the following supplementary services on the Cisco UBE:

- Midcall codec change with voice class codec configuration for SRTP-RTP and SRTP pass-through calls.
• Reinvite-based call hold.
• Reinvite-based call 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.
• Reinvite-based call transfer.
• Call transfer based on a REFER message, with local consumption or pass-through of the REFER message on the Cisco UBE.
• Call forward based on a 302 message, with local consumption or pass-through of the 302 message on the Cisco UBE.
• T.38 fax switchover.
• Fax pass-through switchover.
• DO-EO for SRTP-RTP calls.
• DO-EO for SRTP pass-through calls.

When the initial SRTP-RTP or SRTP pass-through call is established on the Cisco UBE, a call can switch between SRTP and RTP for various supplementary services that can be invoked on the end points. Transcoder resources are used to perform SRTP-RTP conversion on Cisco UBE. When the call switches between SRTP and RTP, the transcoder is dynamically inserted, deleted, or modified. Both normal transcoding and high-density (optimized) transcoding are supported.

For call transfers involving REFER and 302 messages (messages that are locally consumed on Cisco UBE), end-to-end media renegotiation is initiated from Cisco UBE only when you configure the supplementary-service media-renegotiate command in voice service voip configuration mode.

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.

How to Configure Cisco UBE Support for SRTP-RTP Internetworking

Configuring Cisco UBE Support for SRTP-RTP Internetworking

Configuring the Certificate Authority

Perform the steps described in this section to configure the certificate authority.
### SUMMARY STEPS

1. enable
2. configure terminal
3. ip http server
4. crypto pki server `cs-label`
5. database level complete
6. grant auto
7. no shutdown
8. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables the HTTP server on your IPv4 or IPv6 system, including the Cisco web browser user interface.</td>
</tr>
<tr>
<td>ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables a Cisco IOS certificate server and enters certificate server configuration mode.</td>
</tr>
<tr>
<td>crypto pki server <code>cs-label</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• In the example, 3854-cube is specified as the name of the certificate server.</td>
</tr>
<tr>
<td>Device(config)# crypto pki server 3854-cube</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database level complete</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• In the example, each issued certificate is written to the database.</td>
</tr>
<tr>
<td>Device(cs-server)# database level complete</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Trustpoint for the Secure Universal Transcoder

Perform the task in this section to configure, authenticate, and enroll a trustpoint for the secure universal transcoder.

**Before You Begin**

Before you configure a trustpoint for the secure universal transcoder, you should configure the certificate authority, as described in the Configuring the Certificate Authority, on page 321.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. enrollment url url
5. serial-number
6. revocation-check method
7. rsakeypair key-label
8. end
9. crypto pki authenticate name
10. crypto pki enroll name
11. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| Example: | Device> enable |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Device# configure terminal |
| Step 3 | crypto pki trustpoint name | Declares the trustpoint that the router uses and enters ca-trustpoint configuration mode.  
• In the example, the trustpoint is named secdsp. |
| Example: | Device(config)# crypto pki trustpoint secdsp |
| Step 4 | enrollment url url | Specifies the enrollment parameters of a certification authority (CA).  
• In the example, the URL is defined as http://10.13.2.52:80. |
| Example: | Device(ca-trustpoint)# enrollment url http://10.13.2.52:80 |
| Step 5 | serial-number | Specifies whether the router serial number should be included in the certificate request. |
| Example: | Device(ca-trustpoint)# serial-number |
| Step 6 | revocation-check method | Checks the revocation status of a certificate.  
• In the example, the certificate revocation list checks the revocation status. |
| Example: | Device(ca-trustpoint)# revocation-check crl |
| Step 7 | rsakeypair key-label | Specifies which key pair to associate with the certificate.  
• In the example, the key pair 3845-cube generated during enrollment is associated with the certificate. |
| Example: | Device(ca-trustpoint)# rsakeypair 3845-cube |
| Step 8 | end | Exits ca-trustpoint configuration mode. |
| Example: | Device(ca-trustpoint)# end |
### Purpose

#### Command or Action

**Step 9**

`crypto pki authenticate name`

**Example:**

```
Device(config)# crypto pki authenticate secdsp
```

- Authenticates the CA.
  - Accept the trustpoint CA certificate if prompted.

**Step 10**

`crypto pki enroll name`

**Example:**

```
Device(config)# crypto pki enroll secdsp
```

- Obtains the certificate for the router from the CA.
  - Create and enter a new password if prompted.
  - Request a certificate from the CA if prompted.

**Step 11**

`exit`

**Example:**

```
Device(config)# exit
```

- Exits global configuration mode.

### Configuring DSP Farm Services

Perform the task in this section to configure DSP farm services.

**Before You Begin**

Before you configure DSP farm services, you should configure the trustpoint for the secure universal transcoder, as described in the Configuring a Trustpoint for the Secure Universal Transcoder, on page 323.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice-card slot`
4. `dspfarm`
5. `dsp services dspfarm`
6. Repeat Steps 3, 4, and 5 to configure a second voice card.
7. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>voice-card slot</td>
<td>Configures a voice card and enters voice-card configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• In the example, voice card 0 is configured.</td>
</tr>
<tr>
<td>Device(config)# voice-card 0</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>dspfarm</td>
<td>Adds a specified voice card to those participating in a DSP resource pool.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-voicecard)# dspfarm</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>dsp services dspfarm</td>
<td>Enables DSP farm services for a particular voice network module.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-voicecard)# dsp services dspfarm</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td>Repeat Steps 3, 4, and 5 to configure a second voice card.</td>
<td>--</td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits voice-card configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-voicecard)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Associating SCCP to the Secure DSP Farm Profile

Perform the task in this section to associate SCCP to the secure DSP farm profile.

#### Before You Begin

Before you associate SCCP to the secure DSP farm profile, you should configure DSP farm services, as described in the Configuring DSP Farm Services, on page 325.
SUMMARY STEPS

1. enable
2. configure terminal
3. sccp local interface-type interface-number
4. sccp ccm ip-address identifier identifier-number version version-number
5. sccp
6. associate ccm identifier-number priority priority-number
7. associate profile profile-identifier register device-name
8. dspfarm profile profile-identifier transcode universal security
9. trustpoint trustpoint-label
10. codec codec-type
11. Repeat Step 10 to configure required codecs.
12. maximum sessions number
13. associate application sccp
14. no shutdown
15. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sccp local interface-type interface-number</td>
<td>Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco CallManager.</td>
</tr>
<tr>
<td>Example: Device(config)# sccp local GigabitEthernet 0/0</td>
<td>• In the example, the following parameters are set:</td>
</tr>
<tr>
<td></td>
<td>• GigabitEthernet is defined as the interface type that the SCCP application uses to register with Cisco CallManager.</td>
</tr>
<tr>
<td></td>
<td>• The interface number that the SCCP application uses to register with Cisco CallManager is specified as 0/0.</td>
</tr>
<tr>
<td><strong>Step 4</strong> sccp ccm ip-address identifier identifier-number version version-number</td>
<td>Adds a Cisco Unified Communications Manager server to the list of available servers.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Device(config)# sccp ccm 10.13.2.52 identifier 1 version 5.0.1 | • In the example, the following parameters are set:
| | • 10.13.2.52 is configured as the IP address of the Cisco Unified Communications Manager server. |
| | • The number 1 identifies the Cisco Unified Communications Manager server. |
| | • The Cisco Unified Communications Manager version is identified as 5.0.1. |
| **Step 5**  | sccp | Enables SCCP and related applications (transcoding and conferencing) and enters SCCP Cisco CallManager configuration mode. |
|**Example:** | Device(config)# sccp | |
| **Step 6**  | associate ccm identifier-number priority priority-number | Associates a Cisco Unified CallManager with a Cisco CallManager group and establishes its priority within the group. |
|**Example:** | Device(config-sccp-ccm)# associate ccm 1 priority 1 | • In the example, the following parameters are set:
| | • The number 1 identifies the Cisco Unified CallManager. |
| | • The Cisco Unified CallManager is configured with the highest priority within the Cisco CallManager group. |
| **Step 7**  | associate profile profile-identifier register device-name | Associates a DSP farm profile with a Cisco CallManager group. |
|**Example:** | Device(config-sccp-ccm)# associate profile 1 register sxcoder | • In the example, the following parameters are set:
| | • The number 1 identifies the DSP farm profile. |
| | • Sxcoder is configured as the user-specified device name in Cisco Unified CallManager. |
| **Step 8**  | dspfarm profile profile-identifier transcode universal security | Defines a profile for DSP farm services and enters DSP farm profile configuration mode. |
|**Example:** | Device(config-sccp-ccm)# dspfarm profile 1 transcode universal security | • In the example, the following parameters are set:
<p>| | • Profile 1 is enabled for transcoding. |
| | • Profile 1 is enabled for secure DSP farm services. |
| <strong>Step 9</strong>  | trustpoint trustpoint-label | Associates a trustpoint with a DSP farm profile. |
|<strong>Example:</strong> | Device(config-dspfarm-profile)# trustpoint secdsp | • In the example, the trustpoint to be associated with the DSP farm profile is labeled secdsp. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>codec codec-type</strong>&lt;br&gt;Example: <code>Device(config-dspfarm-profile)# codec g711ulaw</code>&lt;br&gt;Specifies the codecs that are supported by a DSP farm profile.&lt;br&gt;• In the example, the g711ulaw codec is specified.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Repeat Step 10 to configure required codecs.---</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>maximum sessions number</strong>&lt;br&gt;Example: <code>Device(config-dspfarm-profile)# maximum sessions 84</code>&lt;br&gt;Specifies the maximum number of sessions that are supported by the profile.&lt;br&gt;• In the example, a maximum of 84 sessions are supported by the profile. The maximum number of sessions depends on the number of DSPs available for transcoding.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>associate application sccp</strong>&lt;br&gt;Example: <code>Device(config-dspfarm-profile)# associate application sccp</code>&lt;br&gt;Associates SCCP to the DSP farm profile.</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>no shutdown</strong>&lt;br&gt;Example: <code>Device(config-dspfarm-profile)# no shutdown</code>&lt;br&gt;Allocates DSP farm resources and associates them with the application.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>exit</strong>&lt;br&gt;Example: <code>Device(config-dspfarm-profile)# exit</code>&lt;br&gt;Exits DSP farm profile configuration mode.</td>
</tr>
</tbody>
</table>

**Registering the Secure Universal Transcoder to the CUBE**

Perform the task in this section to register the secure universal transcoder to the Cisco Unified Border Element. The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature supports both secure transcoders and secure universal transcoders.

**Before You Begin**

Before you register the secure universal transcoder to the Cisco Unified Border Element, you should associate SCCP to the secure DSP farm profile, as described in the Associating SCCP to the Secure DSP Farm Profile, on page 326.
SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. sdspfarm transcode sessions number
5. sdspfarm tag number device-name
6. em logout time1 time2 time3
7. max-ephones max-ephones
8. max-dn max-directory-numbers
9. ip source-address ip-address
10. secure-signaling trustpoint label
11. tftp-server-credentials trustpoint label
12. create cnf-files
13. no sccp
14. sccp
15. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sdspfarm transcode sessions number</td>
<td>Specifies the maximum number of transcoding sessions allowed per Cisco CallManager Express router.</td>
</tr>
<tr>
<td>Example:</td>
<td>• In the example, a maximum of 84 DSP farm sessions are specified.</td>
</tr>
<tr>
<td>Device(config-telephony)# sdspfarm transcode sessions 84</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**Permits a DSP farm to be registered to Cisco Unified CallManager</td>
</tr>
<tr>
<td></td>
<td>Express and associates it with an SCCP client interface's MAC address.</td>
</tr>
<tr>
<td>sdpfarm tag</td>
<td></td>
</tr>
<tr>
<td>number device-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# sdpfarm tag 1 sxcoder</td>
<td>In the example, DSP farm 1 is associated with the sxcoder device.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>**Configures three time-of-day-based timers for automatically logging</td>
</tr>
<tr>
<td></td>
<td>out all Extension Mobility feature users.</td>
</tr>
<tr>
<td>em logout</td>
<td></td>
</tr>
<tr>
<td>time1 time2 time3</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# em logout 0:0 0:0 0:0</td>
<td>In the example, all users are logged out from Extension Mobility after 00:00.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>**Sets the maximum number of Cisco IP phones to be supported by a Cisco</td>
</tr>
<tr>
<td></td>
<td>CallManager Express router.</td>
</tr>
<tr>
<td>max-ephones</td>
<td></td>
</tr>
<tr>
<td>max-ephones</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# max-ephones 4</td>
<td>In the example, a maximum of four phones are supported by the Cisco CallManager Express router.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>**Sets the maximum number of extensions (ephone-dns) to be supported by</td>
</tr>
<tr>
<td></td>
<td>a Cisco Unified CallManager Express router.</td>
</tr>
<tr>
<td>max-dn</td>
<td></td>
</tr>
<tr>
<td>max-directory-numbers</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# max-dn 4</td>
<td>In the example, a maximum of four extensions is allowed.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>**Identifies the IP address and port through which IP phones communicate</td>
</tr>
<tr>
<td></td>
<td>with a Cisco Unified CallManager Express router.</td>
</tr>
<tr>
<td>ip source-address</td>
<td></td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# ip source-address 10.13.2.52</td>
<td>In the example, 10.13.2.52 is configured as the router IP address.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>**Specifies the name of the Public Key Infrastructure (PKI) trustpoint</td>
</tr>
<tr>
<td></td>
<td>with the certificate to be used for TLS handshakes with IP phones on</td>
</tr>
<tr>
<td></td>
<td>TCP port 2443.</td>
</tr>
<tr>
<td>secure-signaling</td>
<td></td>
</tr>
<tr>
<td>trustpoint</td>
<td></td>
</tr>
<tr>
<td>label</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# secure-signaling trustpoint secdsp</td>
<td>In the example, PKI trustpoint secdsp is configured.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>Specifies the PKI trustpoint that signs the phone configuration files.</strong></td>
</tr>
<tr>
<td>tftp-server-credentials trustpoint label</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-telephony)# tftp-server-credentials trustpoint scme</td>
<td>In the example, PKI trustpoint scme is configured.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>create cnf-files</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-telephony)# create cnf-files</td>
</tr>
</tbody>
</table>

| **Step 13** | **no sccp** | Disables SCCP and its related applications (transcoding and conferencing) and exits telephony-service configuration mode. |
| **Example:** | Device(config-telephony)# no sccp |

| **Step 14** | **sccp** | Enables SCCP and related applications (transcoding and conferencing). |
| **Example:** | Device(config)# sccp |

| **Step 15** | **end** | Exits global configuration mode. |
| **Example:** | Device(config)# end |

## Configuring SRTP-RTP Internetworking Support

Perform the task in this section to enable SRTP-RTP internetworking 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.

### Before You Begin

Before you configure the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature, you should register the secure universal transcoder to the Cisco Unified Border Element, as described in the Registering the Secure Universal Transcoder to the CUBE, on page 329.

### Note

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is available only on platforms that support transcoding on the Cisco Unified Border Element. The feature is also available only on secure Cisco IOS images on the Cisco Unified Border Element.
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. srtpt
13. codec codec
14. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Defines a particular dial peer, to specify the method of voice</td>
</tr>
<tr>
<td></td>
<td>• In the example, the following parameters are set:</td>
</tr>
<tr>
<td></td>
<td>• Dial peer 201 is defined.</td>
</tr>
<tr>
<td></td>
<td>• VoIP is shown as the method of encapsulation.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# dial-peer voice 201 voip</td>
</tr>
<tr>
<td><strong>Step 4</strong> destination-pattern string</td>
<td>Specifies either the prefix or the full E.164 telephone number to be</td>
</tr>
<tr>
<td></td>
<td>• In the example, 5550111 is specified as the pattern for the</td>
</tr>
<tr>
<td></td>
<td>• In the example, 5550111 is specified as the pattern for the</td>
</tr>
<tr>
<td></td>
<td>telephone number.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-dial-peer)# destination-pattern 5550111</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>session protocol sipv2</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-dial-peer)# session protocol sipv2</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>session target ipv4: destination-address</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-dial-peer)# session target ipv4:10.13.25.102</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>incoming called-number string</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-dial-peer)# incoming called-number 5550111</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>codec codec</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-dial-peer)# codec g711ulaw</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-dial-peer)#end</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>dial-peer voice tag voip</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# dial-peer voice 200 voip</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>srtp</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-dial-peer)# srtp</code></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>codec codec</code></td>
</tr>
</tbody>
</table>
### Configuring Cisco UBE Support for SRTP-RTP Internetworking

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Device(config-dial-peer)# codec g711ulaw</td>
<td>• In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.</td>
</tr>
</tbody>
</table>

### Step 14

**exit**

**Example:** Device(config-dial-peer)# exit

**Purpose:** Exits dial peer voice configuration mode.

---

**Troubleshooting Tips**

The following commands can help troubleshoot Cisco Unified Border Element support for SRTP-RTP internetworking:

- show crypto pki certificates
- show sccp
- show sdspfarm

**Enabling SRTP on the Cisco UBE**

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 is required for supporting nonsecure supplementary services such as MoH, call forward, and call transfer.

**Enabling SRTP Globally**

Perform this task to enable SRTP globally.

### SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. srtp fallback
5. exit
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode and specifies VoIP encapsulation as the voice-encapsulation type.</td>
</tr>
<tr>
<td>Example: Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> srtp fallback</td>
<td>Enables call fallback to nonsecure mode.</td>
</tr>
<tr>
<td>Example: RoDeviceuter(conf-voi-serv)# srtp fallback</td>
<td>If the secure SIP trunk is towards the Cisco UCM, you must configure the <code>srtp negotiate cisco</code> command in voice-service configuration mode for a non-Cisco fallback to work.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits voice service configuration mode.</td>
</tr>
<tr>
<td>Example: Device(conf-voi-serv)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Enabling SRTP Globally**

```
Device(config)# voice service voip
Device(config-voi-serv)# srtp fallback
Device(config-voi-serv)# exit
```

**Enabling SRTP on a Dial Peer**

Perform this task to enable SRTP on a dial peer.
SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. srtp fallback
5. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Defines a particular dial peer to specify VoIP as the method of voice encapsulation and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# dial-peer voice 10 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> srtp fallback</td>
<td>Enables specific dial-peer calls to fall back to nonsecure mode.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# srtp fallback</td>
<td><strong>Note</strong> If the secure SIP trunk is towards the Cisco UCM, you must configure the <code>srtp negotiate cisco</code> command in dial peer voice configuration mode for a non-Cisco fallback to work.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Enabling SRTP on a Dial Peer**

Device(config)# dial-peer voice 10 voip
Device(config-dial-peer)# srtp fallback
Device(config-dial-peer)# exit
**Troubleshooting Tips**

The following commands can help troubleshoot SRTP-RTP supplementary services support on Cisco UBE:

- `debug ccsip all`
- `debug sccp all`
- `debug voip ccapi inout`

**Verifying SRTP-RTP Supplementary Services Support on the Cisco UBE**

Perform this task to verify the configuration for SRTP-RTP supplementary services support on the Cisco UBE. The `show` commands need not be entered in any specific order.

**SUMMARY STEPS**

1. `enable`
2. `show call active voice brief`
3. `show sccp connection`
4. `show dspfarm dsp active`

**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
Step 3 show sccp connection
Displays SCCP connection details.

Example:


Step 4 show dspfarm dsp active
Displays active DSP information about the DSP farm service.

Example:


Configuration Examples for CUBE Support for SRTP-RTP Internetworking

SRTP-RTP Internetworking Example

The following example shows how to configure Cisco Unified Border Element support for SRTP-RTP internetworking. In this example, the incoming call leg is RTP and the outgoing call leg is SRTP.

enable
configure terminal
ip http server
crypto pki server 3845-cube
database level complete
grant auto
no shutdown
PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically granted.
% 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 1024 bit RSA keys, keys will be non-exportable...[OK]
% SSH-5-ENABLED: SSH 1.99 has been enabled
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
PKI-6-CS_ENABLED: Certificate server now enabled.

crypto pki trustpoint secdsp
enrollment url http://10.13.2.52:80
serial-number
revocation-check crl
rsakeypair 3845-cube
exit

crypto pki authenticate secdsp
Certificate has the following attributes:
 Fingerprint MD5: CCC82E9E 4382CCFE ADA0EBBC 524E2FC1
 Fingerprint SHA1: 34B9C4BF 4841AB31 7B0810AD 80084475 3965F140
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
crypto pki enroll secdsp
Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: 3845-CUBE
% The serial number in the certificate will be: FHK1212F4MU
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
%PKI-6-CERTRET: Certificate received from Certificate Authority

voice-card 0
dspfarm
dsp services dspfarm
voice-card 1
dspfarm
dsp services dspfarm
exit

sccp local GigabitEthernet 0/0
sccp ccm 10.13.2.52 identifier 1 version 5.0.1
scscp
SCCP operational state bring up is successful.sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register sxcoder
dspfarm profile 1 transcode universal security
trustpoint secdsp
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec ilbc
codec g729br8
maximum sessions 84
associate application sccp
no shutdown
exit

telephony-service
Feature Information for CUBE Support for SRTP-RTP Internetworking

Table 29: Feature Information for Cisco Unified Border Element Support for SRTP-RTP Internetworking

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Border Element Support for SRTP-RTP Internetworking</td>
<td>12.4(22)YB, 15.0(1)M</td>
<td>This feature allows secure enterprise-to-enterprise calls. Support for SRTP-RTP internetworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls. The following sections provide information about this feature: The following command was introduced: <code>tls</code>.</td>
</tr>
</tbody>
</table>
The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplementary Services Support on Cisco UBE for RTP-SRTP Calls</td>
<td>15.2(1)T</td>
<td>The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.</td>
</tr>
<tr>
<td>Supplementary Services Support on Cisco UBE for RTP-SRTP Calls</td>
<td>Cisco IOS XE Release 3.7S</td>
<td>The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.</td>
</tr>
</tbody>
</table>
Support for SRTP Termination

This Support for SRTP Termination feature enables Cisco Unified Border Element (Cisco UBE) support for Secure Real-time Transport Protocol (SRTP) on the Session Initiation Protocol (SIP) Trunk interface.

- Finding Feature Information, page 343
- Information About Support for SRTP Termination, page 343
- How to Configure Support for SRTP Termination, page 346
- Verifying Support for SRTP Termination, page 348
- Configuration Examples for Support for SRTP Termination, page 349
- Additional References for Support for SRTP Termination, page 350
- Feature Information for Support for SRTP Termination, page 350

Finding Feature Information

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

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

Information About Support for SRTP Termination

The Support for SRTP Termination feature configures Cisco Unified Border Element (Cisco UBE) support for an Secure Real-time Transport Protocol (SRTP) connection using the AES_CM_128_HMAC_SHA1_80 crypto suite. This feature implements crypto-suite negotiation and appropriately sets up the call on the following two sides:

- The Cisco Unified Call Manager (CUCM) or IP phones side—Connection between the end devices and CUBE
• SIP Trunk side—Connection between CUBE and Service Provider

Prior to the Support for SRTP Termination feature, Cisco UBE could support an SRTP connection using the AES_CM_128_HMAC_SHA1_32 crypto suite. This crypto suite is still used by default, unless Cisco UBE is configured to use AES_CM_128_HMAC_SHA1_80 crypto suite.

Cisco UBE SRTP termination can be implemented in the following ways:

• SRTP-RTP interworking—This method is used with devices (CUCM or IP Phone devices) that still support AES_CM_128_HMAC_SHA1_32 crypto suite only.

• SRTP-SRTP pass-through—This method is used with devices that support AES_CM_128_HMAC_SHA1_80 crypto suite.

---

**Note**

This method of implementation is currently supported by non-CUCM end devices like Microsoft Link. This method can also be used when CUCM or IP phone devices support AES_CM_128_HMAC_SHA1_80 crypto suite.

---

**For End Devices Supporting AES_CM_128_HMAC_SHA1_80 Crypto Suite**

This method is used between Cisco Unified Border Element (Cisco UBE), IP Phones, and other Cisco Unified Call Manager (CUCM) devices that support AES_CM_128_HMAC_SHA1_80 crypto suite.

• CUCM or IP Phones side—A Secure Real-time Transport Protocol (SRTP) connection using the AES_CM_128_HMAC_SHA1_80 crypto suite exists here. In the figure below, IP Phone and CUBE within the customer network connect with an SRTP connection using AES_CM_128_HMAC_SHA1_80 crypto suite.

• Session Initiation Protocol (SIP) Trunk side—An SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite. In the figure below, CUBE on the Customer Network
and SBC on the Service Provider Network connect with an SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite.

**Figure 23: SRTP Connection Supporting AES_CM_128_HMAC_SHA1_80 crypto suite**

![Diagram showing SRTP connection](image)

**For End Devices Supporting AES_CM_128_HMAC_SHA1_32 Crypto Suite**

A single Cisco Unified Call Manager (Cisco UBE) 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 Cisco UBE device with the AES_CM_128_HMAC_SHA1_80 crypto suite at the same time.

For Cisco Unified Call Manager (CUCM) 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.

- CUCM 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 24: SRTP-RTP Interworking Supporting AES_CM_128_HMAC_SHA1_32 crypto suite

How to Configure Support for SRTP Termination

Configuring Crypto Authentication

Configuring Crypto Authentication (Global Level)

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. srtp-auth {sha1-32 | sha1-80}
6. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>enable</th>
<th>Enables privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
<th>Enters global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>voice service voip</th>
<th>Specifies VoIP encapsulation and enters voice-service configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(config)# voice service voip</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>sip</th>
<th>Enters the Session Initiation Protocol (SIP) configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(conf-voi-serv)# sip</td>
<td></td>
</tr>
</tbody>
</table>

| Step 5 | srtp-auth {sha1-32 | sha1-80} | Configures an SRTP connection on CUBE using the preferred crypto suite. |
|--------|---------------------------------|---------------------------------------------------------------------|
| Example: | Device(conf-serv-sip)# srtp-auth sha1-80 |

<table>
<thead>
<tr>
<th>Step 6</th>
<th>end</th>
<th>Ends the current configuration session and returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(conf-serv-sip)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Crypto Authentication (Dial Peer Level)

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip srtp-auth {sha1-32 | sha1-80 | system}
5. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>dial-peer voice tag voip</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# dial-peer voice 15 voip</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Defines a VoIP dial peer and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>voice-class sip srtp-auth {sha1-32</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-dial-peer)# voice-class sip srtp-auth sha1-80</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures an SRTP connection on CUBE using the preferred crypto suite.</td>
</tr>
<tr>
<td></td>
<td>• The default value is sha1-32.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-serv-sip)# end</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Verifying Support for SRTP Termination

Perform this task to verify the configuration of an SRTP connection on Cisco Unified Border Element using the AES_CM_128_HMAC_SHA1_80 crypto suite. The show commands can be entered in any order.

SUMMARY STEPS

1. show sip-ua calls
2. show sip-ua srtp

DETAILED STEPS

**Step 1**

show sip-ua calls

**Example:**
The following example displays sample output for active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls:

Device# show sip-ua calls
Call 1
SIP Call ID : 20894
   Media Stream 1
      Local Crypto Suite : AES_CM_128_HMAC_SHA1_80
      Remote Crypto Suite: AES_CM_128_HMAC_SHA1_80 (AES_CM_128_HMAC_SHA1_32

Step 2 show sip-ua srtp

Example:
The following example displays sample output for Session Initiation Protocol (SIP) user-agent (UA) SRTP information:

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

Configuration Examples for Support for SRTP Termination

Example: Configuring Crypto Authentication

Example: Configuring Crypto Authentication (Global Level)

The following example shows how to configure Cisco UBE 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(config-voi-serv)# sip
Device(config-serv-sip)# srtp-auth sha1-80
Device(config-serv-sip)# end

Example: Configuring Crypto Authentication (Dial Peer Level)

The following example shows how to configure Cisco UBE 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
Additional References for Support for SRTP Termination

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>SIP configuration tasks</td>
<td>SIP Configuration Guide, Cisco IOS Release 15M&amp;T</td>
</tr>
</tbody>
</table>

Technical Assistance

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

Feature Information for Support for SRTP Termination

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 30: Feature Information for Support for SRTP Termination

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for SRTP Termination</td>
<td>Cisco IOS XE Release 3.11S</td>
<td>The Support for SRTP Termination feature describes how to configure Cisco Unified Border Element to support AES_CM_128_HMAC_SHA1_80 crypto suite on the Session Initiation Protocol (SIP) Trunk interface. The following commands were introduced or modified: <em>show sip-ua srtp</em>, <em>srtp-auth</em> and <em>voice-class sip srtp-auth</em>.</td>
</tr>
</tbody>
</table>
WebEx Telepresence Media Support Over Single SIP Session

The WebEx Telepresence Media Support over Single SIP Session feature provides support for end-to-end negotiation of up to 6 m-lines or media lines over a single Session Initiation Protocol (SIP) session. The media types can be audio, video, or application.

- Finding Feature Information, page 353
- Restrictions for WebEx Telepresence Media Support Over Single SIP Session, page 353
- Information About WebEx Telepresence Media Support Over Single SIP Session, page 354
- Monitoring WebEx Telepresence Media Support Over Single SIP Session, page 354
- Feature Information for WebEx Telepresence Media Support Over Single SIP Session, page 357

Finding Feature Information

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

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

Restrictions for WebEx Telepresence Media Support Over Single SIP Session

- High availability is not supported with multiple m-lines.
- Only single dynamic payload type in the m-line for H.224 protocol is supported.
- Payload type interworking for Aggregation Service Routers (ASR) is not supported, so dynamic payload type is negotiated end-to-end.
Information About WebEx Telepresence Media Support Over Single SIP Session

The WebEx Telepresence Media Support over Single SIP Session feature provides the following support:

- End-to-end negotiation of multiple m-lines.
- Negotiation of Binary Floor Control Protocol (BFCP), IX, and H.224 protocol m-lines (m=application) and creation of Real-time Transport Protocol (RTP) or UDP streams for the same.
- Early-Offer (EO-EO) and Delayed-Offer (DO-DO) calls' support by the Cisco Unified Border Element (Cisco UBE) with multiple m-lines.
- End-to-end negotiation of multiple m-lines of same media type for video and application (but not audio).
- Mid-call escalation and de-escalation for multiple application and video m-lines.
- Secure RTP (SRTP) passthrough for all RTP streams (audio, video, and application).
- SRTP-RTP interworking for video (ASR only).
- Multiple dynamic payload types in the same m-line for the H.264 codec.

You can use the `show voip rtp connections` and `show call active video compact` commands to see the details about additional video and application streams.

Monitoring WebEx Telepresence Media Support Over Single SIP Session

Perform this task to see the details about additional video and application streams. The `show` commands can be entered in any order.

**SUMMARY STEPS**

1. `enable`
2. `show call active video compact`
3. `show voip rtp connections`
4. `show sip-ua calls`

**DETAILED STEPS**

**Step 1** `enable`

Enables privileged EXEC mode.

**Example:**

```
Device> enable
```
Step 2  show call active video compact
Displays a compact version of call information for Skinny Call Control Protocol (SCCP), SIP, and H.323 video calls in progress. The codec type, negotiated codec, and remote media ports are displayed.

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
1 ANS T5 H264 VOIP-VIDEO P332211 9.45.38.39:2448
6 ORG T5 H264 VOIP-VIDEO P1111 9.45.38.39:2438

Step 3  show voip rtp connections
Displays RTP named event packets. In the following sample output, two RTP connections are displayed for each m-line and a total of 10 RTP connections are displayed for 5 m-lines.

Example:
Device# show voip rtp connections
VoIP RTP active connections :
No. CallId dstCallId LocalRTP RmtRTP LocalIP RemoteIP
1 1 6 16384 54024 192.0.2.123 192.0.2.39
2 2 7 16386 2448 192.0.2.123 192.0.2.39
3 3 8 16400 5070 192.0.2.123 192.0.2.39
4 4 9 16388 2450 192.0.2.123 192.0.2.39
5 5 10 16402 2452 192.0.2.123 192.0.2.39
6 6 1 16390 58121 192.0.2.123 192.0.2.39
7 7 2 16392 2438 192.0.2.123 192.0.2.39
8 8 3 16394 5070 192.0.2.123 192.0.2.39
9 9 4 16396 2440 192.0.2.123 192.0.2.39
10 10 5 16398 2442 192.0.2.123 192.0.2.39
Found 10 active RTP connections

Step 4  show sip-ua calls
Displays active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (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 : 72B6C784-753E11E2-FFFFFFFF8008B555-FFFFFFFFE340699E@9.45.47.123
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 332211
Called Number : 1111
Bit Flags : 0xC04018 0x10000100 0x80
CC Call ID : 6
Source IP Address (Sig ) : 9.45.47.123
Destn SIP Req Addr:Port : [9.45.38.39]:5267
Destn SIP Resp Addr:Port : [9.45.38.39]:5267
Destination Name : 9.45.38.39
Number of Media Streams : 5
Number of Active Streams: 5
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)
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: [9.45.47.123]:16390
Media Dest IP Addr:Port : [9.45.38.39]:58121

Media Stream 2
State of the stream : STREAM_ACTIVE
Stream Call ID : 7
Stream Type : video (7)
Stream Media Addr Type : 1
Negotiated Codec : h263 (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: [9.45.47.123]:16392
Media Dest IP Addr:Port : [9.45.38.39]:2438

Media Stream 3
State of the stream : STREAM_ACTIVE
Stream Call ID : 8
Stream Type : application (8)
Stream Media Addr Type : 1
Negotiated Codec : No Codec (0 bytes)
Codec Payload Type : 255 (None)
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: [9.45.47.123]:16394
Media Dest IP Addr:Port : [9.45.38.39]:5070

Media Stream 4
State of the stream : STREAM_ACTIVE
Stream Call ID : 9
Stream Type : video (7)
Stream Media Addr Type : 1
Negotiated Codec : h263 (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: [9.45.47.123]:16396
Media Dest IP Addr:Port : [9.45.38.39]:2440

Media Stream 5
State of the stream : STREAM_ACTIVE
Stream Call ID : 10
Stream Type : application (8)
Stream Media Addr Type : 1
Negotiated Codec : H.224 (0 bytes)
Codec Payload Type : 107
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Feature Information for WebEx Telepresence Media Support Over Single SIP 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 31: Feature Information for WebEx Telepresence Media Support Over Single SIP Session

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebEx Telepresence Media Support Over Single SIP Session</td>
<td>15.3(2)T</td>
<td>The WebEx Telepresence Media Support over Single SIP Session feature provides support for end-to-end negotiation of up to 6 m-lines or media lines over a single Session Initiation Protocol (SIP) session. The media types can be audio, video, or application.</td>
</tr>
<tr>
<td>WebEx Telepresence Media Support Over Single SIP Session</td>
<td>Cisco IOS XE Release 3.9S</td>
<td>The WebEx Telepresence Media Support over Single SIP Session feature provides support for end-to-end negotiation of up to 6 m-lines or media lines over a single Session Initiation Protocol (SIP) session. The media types can be audio, video, or application.</td>
</tr>
</tbody>
</table>
Feature Information for WebEx Telepresence Media Support Over Single SIP Session
SIP SRTP Fallback to Nonsecure RTP

The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from Secure Real-time Transport Protocol (SRTP) to Real-time Transport Protocol (RTP) by accepting or sending an RTP/Audio-Video Profile (AVP) (RTP) profile in response to an RTP/SAVP (SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure Transport Layer Security (TLS), IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes.

- Finding Feature Information, page 359
- Prerequisites for SIP SRTP Fallback to Nonsecure RTP, page 359
- Configuring SIP SRTP Fallback to Nonsecure RTP, page 360
- Feature Information for SIP SRTP Fallback to Nonsecure RTP, page 360

Finding Feature Information

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

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

Prerequisites for SIP SRTP Fallback to Nonsecure RTP

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)T or a later release must be installed and running on your Cisco Unified Border Element.
Cisco Unified Border Element (Enterprise)

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

Configuring SIP SRTP Fallback to Nonsecure RTP

To enable this feature, see the "Configuring SIP Support for SRTP" section of the Cisco IOS SIP Configuration Guide, Release 15.1 at the following URL:


Detailed command information for the `srtp`, `srtp negotiate`, and `voice-class sip srtp negotiate` commands is located in the Cisco IOS Voice Command Reference


Feature Information for SIP SRTP Fallback to Nonsecure RTP

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 SIP SRTP Fallback to Nonsecure RTP**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP SRTP Fallback to Nonsecure RTP</td>
<td>12.4(22)T</td>
<td>The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from SRTP to RTP by accepting or sending an RTP/AVP(RTP) profile in response to an RTP/SAVP(SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure TLS, IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes. The following commands were introduced or modified: <code>srtp (voice)</code>, <code>srtp negotiate</code>, and <code>voice-class sip srtp negotiate</code></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>SIP SRTP Fallback to Nonsecure RTP</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from SRTP to RTP by accepting or sending an RTP/AVP(RTP) profile in response to an RTP/SAVP(SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure TLS, IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes. The following commands were introduced or modified: <code>srtp (voice)</code>, <code>srtp negotiate</code>, and <code>voice-class sip srtp negotiate</code></td>
</tr>
</tbody>
</table>
Support for Software Media Termination Point

The Support for Software Media Termination Point (MTP) feature bridges the media streams between two connections allowing Cisco Unified Communications Manager (Cisco UCM) to relay calls that are routed through SIP or H.323 endpoints via Skinny Call Control Protocol (SCCP) commands. These commands allow Cisco UCM to establish an MTP for call signaling.

- Finding Feature Information, page 363
- Information About Support for Software Media Termination Point, page 363
- How to Configure Support for Software Media Termination Point, page 364
- Prerequisites, page 364
- Restrictions, page 364
- Configuring Support for Software Media Termination Point, page 364
- Feature Information for Support for Software Media Termination Point, page 369

Finding Feature Information

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

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

Information About Support for Software Media Termination Point

This feature extends the software MTP support to the Cisco Unified Border Element (Enterprise). Software MTP is an essential component of large-scale deployments of Cisco UCM. This feature enables new capabilities
so that the Cisco UBE can function as an Enterprise Edge Cisco Session Border Controller for large-scale deployments that are moving to SIP trunking.

How to Configure Support for Software Media Termination Point

Prerequisites

• For the software MTP to function properly, codec and packetization must be configured the same way on both in call legs and out call legs.

Cisco Unified Border Element (Enterprise)

• Cisco IOS XE Release 2.6 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

• RSVP Agent is not supported in software MTP.
• Hardware MTP for repacketization is not supported.
• Call Threshold is not supported for standalone software MTP.
• Per-call debugging is not supported.

Configuring Support for Software Media Termination Point

To enable and configure the Support for Software Media Termination Point feature, perform the following task.
SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sccp local interface-type interface-number [port port-number]`
4. `sccp ccm {ipv4-address | ipv6-address | dns} identifier identifier-number [port port-number] version version-number`
5. `sccp`
6. `sccp ccm group group-number`
7. `associate ccm identifier-number priority number`
8. `associate profile profile-identifier register device-name`
9. `dsfp rpc profile profile-identifier {conference | mtp | transcode} [security]`
10. `maximum sessions {hardware | software} number`
11. `associate application sccp`
12. `no shutdown`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>· Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sccp local interface-type interface-number [port port-number]</td>
<td>Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco UCM.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# sccp local gigabitethernet0/0/0</code></td>
<td>· <code>interface type</code> -- Can be an interface address or a virtual-interface address such as Ethernet.</td>
</tr>
<tr>
<td></td>
<td>· <code>interface number</code> -- Interface number that the SCCP application uses to register with Cisco UCM.</td>
</tr>
<tr>
<td></td>
<td>· (Optional) <code>port port-number</code> -- Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.</td>
</tr>
<tr>
<td><strong>Step 4</strong> sccp ccm {ipv4-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td></td>
<td>· <code>ipv4-address</code> -- IP version 4 address of the Cisco UCM server.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+` | • *ipv6-address* --IP version 6 address of the Cisco UCM server.  
• *dns* --DNS name.  
• *identifier* --Specifies the number that identifies the Cisco UCM server. Range is 1 to 65535.  
• *port* *port-number* (Optional) --Specifies the TCP port number. Range is 1025 to 65535. Default is 2000.  
• *version* *version-number* --Cisco UCM version. Valid versions are 3.0, 3.1, 3.2, 3.3, 4.0, 4.1, 5.0.1, 6.0, and 7.0+. There is no default value. |

**Step 5**  
**sccp**  
**Example:**  
`Router(config)# sccp`  
Enables the Skinny Client Control Protocol (SCCP) and its related applications (transcording and conferencing).

**Step 6**  
**sccp ccm group** *group-number*  
**Example:**  
`Router(config)# sccp ccm group 10`  
Creates a Cisco UCM group and enters SCCP Cisco UCM configuration mode.  
• *group-number* --Identifies the Cisco UCM group. Range is 1 to 50.

**Step 7**  
**associate ccm** *identifier-number* *priority number*  
**Example:**  
`Router(config-sccp-ccm)# associate ccm 10 priority 3`  
Associates a Cisco UCM with a Cisco UCM group and establishes its priority within the group:  
• *identifier-number* --Identifies the Cisco UCM. Range is 1 to 65535. There is no default value.  
• *priority number* --Priority of the Cisco UCM within the Cisco UCM group. Range is 1 to 4. There is no default value. The highest priority is 1.

**Step 8**  
**associate profile** *profile-identifier* **register device-name**  
**Example:**  
`Router(config-sccp-ccm)# associate profile 1 register MTP0011`  
Associates a DSP farm profile with a Cisco UCM group:  
• *profile-identifier* --Identifies the DSP farm profile. Range is 1 to 65535. There is no default value.  
• *register device-name* --Device name in Cisco UCM. A maximum of 15 characters can be entered for the device name.

**Step 9**  
**ds pfarm profile** *profile-identifier*  
{conference | mtp | transcode | [security]}  
**Example:**  
`Router(config-sccp-ccm)# ds pfarm profile 1 mtp`  
Enters DSP farm profile configuration mode and defines a profile for DSP farm services:  
• *profile-identifier* --Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.  
• *conference* --Enables a profile for conferencing.  
• *mtp* --Enables a profile for MTP.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• transcode</td>
<td>— Enables a profile for transcoding.</td>
</tr>
<tr>
<td>• security (Optional)</td>
<td>— Enables a profile for secure DSP farm services.</td>
</tr>
</tbody>
</table>

**Step 10**

<table>
<thead>
<tr>
<th>maximum sessions {hardware</th>
<th>software} number</th>
</tr>
</thead>
</table>

**Example:**

```bash
Router(config-dspfarm-profile)#
maximum sessions software 10
```

Specifies the maximum number of sessions that are supported by the profile.

- **hardware** — Number of sessions that MTP hardware resources can support.
- **software** — Number of sessions that MTP software resources can support.
- **number** — Number of sessions that are supported by the profile. Range is 0 to \( x \). Default is 0. The \( x \) value is determined at runtime depending on the number of resources available with the resource provider.

**Step 11**

<table>
<thead>
<tr>
<th>associate application sccp</th>
</tr>
</thead>
</table>

**Example:**

```bash
Router(config-dspfarm-profile)#
associate application sccp
```

Associates SCCP to the DSP farm profile.

**Step 12**

<table>
<thead>
<tr>
<th>no shutdown</th>
</tr>
</thead>
</table>

**Example:**

```bash
Router(config-dspfarm-profile)#
no shutdown
```

Changes the status of the interface to the UP state.

### Examples

The following example shows a sample configuration for the Support for Software Media Termination Point feature:

```bash
sccp local GigabitEthernet0/0/1
sccp ccm 10.13.40.148 identifier 1 version 6.0
sccp
!
sccp ccm group 1
bind interface GigabitEthernet0/0/1
associate ccm 1 priority 1
associate profile 6 register RR_RLS6
!
dspfarm profile 6 mtp
codec g711ulaw
maximum sessions software 100
associate application SCCP
!
```
Troubleshooting Tips

To verify and troubleshoot this feature, use the following show commands:

- To verify information about SCCP, use the show sccp command:

Router# show sccp
SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.13.40.146, Port Number: 2000
    Priority: N/A, Version: 6.0, Identifier: 1
    Trustpoint: N/A

- To verify information about the DSPfarm profile, use the show dspfarm profile command:

Router# show dspfarm profile 6
Dspfarm Profile Configuration
Profile ID = 6, Service = MTP, Resource ID = 1
Profile Description:
Profile Service Mode : Non Secure
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP Status : ASSOCIATED
Resource Provider : NONE Status : NONE
Number of Resource Configured : 100
Number of Resource Available : 100
Hardware Configured Resources : 0
Hardware Available Resources : 0
Software Resources : 100
Codec Configuration
Codec : g711ulaw, Maximum Packetization Period : 30

- To display statistics for the SCCP connections, use the show sccp connections command:

Router# show sccp connections
sess_id conn_id stype mode codec ripaddr rport sport  
16808048 16789079 mtp sendrecv g711u 10.13.40.20 17510 7242  
16808048 16789078 mtp sendrecv g711u 10.13.40.157 6900 18050

- To display information about RTP connections, use the show rtpspi call command:

Router# show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode LocalRTP RmtRTP LocalIP RemoteIP SRTP  
22 19 Snd-Rcv 7242 17510 0x90D080F 0x90D0814 0  
19 22 Snd-Rcv 18050 6900 0x90D080F 0x90D080F 0

- To display information about VoIP RTP connections, use the show voip rtp connections command:

Router# show voip rtp connections
VoIP RTP Port Usage Information
Max Ports Available: 30000, Ports Reserved: 100, Ports in Use: 102
Port range not configured, Min: 5500, Max: 65499
VoIP RTP active connections:

<table>
<thead>
<tr>
<th>No.</th>
<th>CallId</th>
<th>dstCallId</th>
<th>LocalRTP</th>
<th>RmtRTP</th>
<th>LocalIP</th>
<th>RemoteIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>114</td>
<td>117</td>
<td>19822</td>
<td>24556</td>
<td>10.13.40.157</td>
<td>10.13.40.157</td>
</tr>
<tr>
<td>3</td>
<td>116</td>
<td>115</td>
<td>19176</td>
<td>52625</td>
<td>10.13.40.157</td>
<td>10.13.40.20</td>
</tr>
<tr>
<td>4</td>
<td>117</td>
<td>114</td>
<td>16526</td>
<td>52624</td>
<td>10.13.40.157</td>
<td>10.13.40.20</td>
</tr>
</tbody>
</table>

- Additional, more specific, `show` commands that can be used include the following:
  - `show sccp connection callid`
  - `show sccp connection connid`
  - `show sccp connection sessionid`
  - `show rtpspi call callid`
  - `show rtpspi stat callid`
  - `show voip rtp connection callid`
  - `show voip rtp connection type`

- To isolate specific problems, use the `debug sccp` command:
  - `debug sccp [all | config | errors | events | keepalive | messages | packets | parser | tls]`

---

**Feature Information for Support for Software Media Termination Point**

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Feature History Table for the ASR**

**Table 33: Feature Information for Support for Software Media Termination Point**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Software Media Termination Point</td>
<td>Cisco IOS XE Release 2.6 S</td>
<td>Software Media Termination Point (MTP) provides the capability for Cisco Unified Communications Manager (Cisco UCM) to interact with a voice gateway via Skinny Client Control Protocol (SCCP) commands. These commands allow the Cisco UCM to establish an MTP for call signaling.</td>
</tr>
</tbody>
</table>
Cisco Unified Communication Trusted Firewall Control

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. Firewall traversal is accomplished using Session Traversal Utilities for NAT (STUN) on a TRP collocated with a Cisco Unified Communications Manager Express (Cisco Unified CME) or a Cisco Unified Border Element.

- Finding Feature Information, page 371
- Prerequisites, page 371
- Configuring Cisco Unified Communication Trusted Firewall Control, page 372
- Feature Information for Cisco Unified Communication Trusted Firewall Control, page 372

Finding Feature Information

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

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

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)T or a later release must be installed and running on your Cisco Unified Border Element.
Cisco Unified Border Element (Enterprise)

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

Configuring Cisco Unified Communication Trusted Firewall Control

To enable this feature, see the "Cisco Unified Communications Trusted Firewall Control" feature guide. Detailed command information for the `stun`, `stun flowdata agent-id`, `stun flowdata keepalive`, `stun flowdata shared-secret`, `stun usage firewall-traversal flowdata`, `voice-class stun-usage` commands is located in the Cisco IOS Voice Command Reference.

Feature Information for Cisco Unified Communication Trusted Firewall Control

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Trusted Firewall Control</td>
<td>12.4(22)T</td>
<td>Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following commands were introduced or modified: <code>stun</code>, <code>stun flowdata agent-id</code>, <code>stun flowdata keepalive</code>, <code>stun flowdata shared-secret</code>, <code>stun usage firewall-traversal flowdata</code>, <code>voice-class stun-usage</code>.</td>
</tr>
</tbody>
</table>
Table 35: Feature Information for Cisco Unified Communication Trusted Firewall Control

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Trusted Firewall Control</td>
<td>Cisco IOS XE Release 3.3S</td>
<td>Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following commands were introduced or modified: stun, stun flowdata agent-id, stun flowdata keepalive, stun flowdata shared-secret, stun usage firewall-traversal flowdata, voice-class stun-usage.</td>
</tr>
</tbody>
</table>
Cisco Unified Communication Trusted Firewall Control-Version II

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. TRP is a Cisco IOS service feature, which is similar to the Resource Reservation Protocol (RSVP) agent. Firewall traversal is accomplished using Session Traversal Utilities for NAT (STUN) on a TRP colocated with a Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Unified Border Element, and Media Termination Points (MTP).

This release introduces the following features:

- Noncolocated firewall for UC SIP trunks
- Support Firewall traversal for Cisco Unified Border Element call flows in which the media flow through the Media Termination Points such as MTP, Transcoder, or Conference bridge with Trust Relay Point (TRP) enabled.
- Firewall traversal for additional Cisco Unified Border Element call flows using STUN.

Finding Feature Information, page 375
Prerequisites for Cisco Unified Communication Trusted Firewall Control-Version II, page 376
Configuring Cisco Unified Communication Trusted Firewall Control-Version II, page 376
Feature Information for Cisco Unified Communication Trusted Firewall Control-Version II, page 376

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for Cisco Unified Communication Trusted Firewall Control-Version II

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Configuring Cisco Unified Communication Trusted Firewall Control-Version II

To enable this feature, see the "Cisco Unified Communications Trusted Firewall Control-Version II" feature guide.

Detailed command information for the `stun flowdata catlife` command is located in the Cisco IOS Voice Command Reference.

Feature Information for Cisco Unified Communication Trusted Firewall Control-Version II

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communication Trusted Firewall Control-Version II</td>
<td>15.0(1)T</td>
<td>Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following command was introduced: <code>stun flowdata catlife</code>.</td>
</tr>
</tbody>
</table>
Table 37: Feature Information for Cisco Unified Communication Trusted Firewall Control-Version II

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communication Trusted Firewall Control-Version II</td>
<td>Cisco IOS XE Release 3.3S</td>
<td>Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following command was introduced: <strong>stun flowdata catlife</strong>.</td>
</tr>
</tbody>
</table>
CHAPTER 34

Finding Feature Information

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

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

• Prerequisites for Cisco Unified Communications Trusted Firewall Control - Version III, page 379
• Restrictions for Enhanced Firewall Traversal for Cisco Unified Communications, page 380
• Information About Cisco Unified Communications Trusted Firewall Control - Version III, page 380
• How to Configure Cisco Unified Communications Trusted Firewall Control - Version III, page 383
• Feature Information for Cisco Unified Communications Trusted Firewall Control - Version III, page 398

Prerequisites for Cisco Unified Communications Trusted Firewall Control - Version III

• Ensure that you have the correct platform to support this feature. Cisco Unified Communications Trusted Firewall Control is supported on the Cisco 1861, 2801, 2811, 2821, 2851, 3825, and 3845 platforms.
• Cisco IOS Release 15.1(2)T
• All k9 images with voice support. Session Timer feature can run on any voice image and does not support the firewall traversal.
• uc-base and securityk9 licenses on Cisco 29xx and 39xx platforms. Session Timer feature does not require securityk9 licenses.

Configuration Prerequisites

The trusted firewall traversal for Cisco Unified CME SIP line side endpoints can be configured using TRP. The TRP must be configured under voice service voip> stun with the following information:
Restrictions for Enhanced Firewall Traversal for Cisco Unified Communications

Cisco IOS Release 15.1(2)T implements firewall traversal for media using STUN on TRP and is not supported for:

- RSVP flow support through the Firewall
- Traditional SRST mode
- H.323 trunk support for Unified Communication Trusted Firewall
- Media flow around on Cisco Unified Border Element
- IPv6
- IP Multicast
- Video calls on SCCP and SIP line side

Information About Cisco Unified Communications Trusted Firewall Control - Version III

Before you configure Enhanced Firewall Traversal using STUN, you should understand the following concepts:

Overview of Firewall Traversal for Cisco Unified Communications

In previous releases, firewall traversal implemented a new framework for IOS firewall traversal on Cisco Unified CME and Cisco Unified Border Element for SIP trunks.

For more information on Cisco trusted firewall traversal, see:
SIP Session Timer

The SIP Session Timer (RFC 4028) is the standard SIP keepalive mechanism that keeps the SIP session active. The SIP user agents send periodic re-INVITE or UPDATE requests (referred to as session refresh requests) to keep the session alive. The interval for the session refresh request is determined through a negotiation mechanism. Session Timer is used to allow SIP signaling through the IOS firewall. You must configure Access Control List (ACL) or partial SIP-Application Layer Gateway (ALG) on the Cisco IOS firewall to allow SIP signaling.

After signaling, a pinhole is created. The firewall starts an inactivity timer, so that in case the user agents crashes or reboots during the call or the BYE message is lost, it can remove its states when the timer starts.

For the Cisco Unified CME SIP line side, by default, the endpoint sends periodic REGISTER messages on port 5060.

- A partial SIP-ALG keeps track of the endpoint registration and keeps the signaling pinhole open as far as the registration is active.
- An ACL tracks the User Datagram Protocol (UDP) / Transmission Control Protocol (TCP) messages that travel across the signaling port and keeps the signaling pinhole open.

However, the Cisco Unified CME SIP trunks do not exchange periodic SIP messages. The Cisco IOS firewall control sessions times out if no SIP messages are exchanged. The timed out SIP over UDP sessions are re-established with the next SIP message (for example, BYE). Timed out SIP over TCP sessions are not re-established and the subsequent SIP messages (for example, BYE) will be dropped.

Restrictions and Limitations for SIP Session Timer

SIP session timer does not support the following:

- Media modifications in responses to locally sent ReINVITE for session refresh
- Session timer in early dialog UPDATE

SIP Session Timer on CUBE for SIP-SIP Call Flows

The following table shows who will be sending the session refresh requests for all combinations of User Agent Clients (UAC) / User Agent Server (UAS) support for session timer

<table>
<thead>
<tr>
<th>S.No</th>
<th>UAC Support</th>
<th>UAS Support</th>
<th>Command Line Interface Enabled on IN leg</th>
<th>Command Line Interface Enabled on OUT leg</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>UAC/UAS will send the session refresh requests and the Call Control Agent will pass it across.</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>S.No</td>
<td>UAC Support</td>
<td>UAS Support</td>
<td>Command Line Interface Enabled on IN leg</td>
<td>Command Line Interface Enabled on OUT leg</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>4</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>UAC/UAS may send session refresh requests and the Call Control Agent will pass it across.</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>If the incoming INVITE has no &quot;refresher&quot; or &quot;refresher=ua&quot;, UAC will send the session refresh requests and the Call Control Agent will pass it across. The Call Control Agent will also start the session expiration timer on the IN LEG.</td>
</tr>
<tr>
<td>6</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>If the incoming INVITE has &quot;refresher=uas&quot;, the Call Control Agent will send the session refresh requests on the appropriate leg(s).</td>
</tr>
<tr>
<td>7</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>UAC may send the session refresh requests and the Call Control Agent will pass it across.</td>
</tr>
<tr>
<td>8</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>If the 2xx response from UAS has &quot;refresher=ua&quot;, UAS will send the session refresh requests and the Call Control Agent will pass it across. The Call Control Agent will also start the session expiration timer on the OUT LEG.</td>
</tr>
<tr>
<td>9</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>If the 2xx response from UAS has no &quot;refresher&quot; or has &quot;refresher=ua&quot;, the Call Control Agent will send the session refresh requests on the appropriate call leg(s).</td>
</tr>
<tr>
<td>10</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>UAS may send the session refresh requests and the Call Control Agent will pass it across.</td>
</tr>
<tr>
<td>11</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Call Control Agent will send the session refresh requests on the appropriate call leg(s).</td>
</tr>
<tr>
<td>12</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No session timer.</td>
</tr>
<tr>
<td>13</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No session timer.</td>
</tr>
<tr>
<td>14</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No session timer.</td>
</tr>
<tr>
<td>15</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No session timer.</td>
</tr>
<tr>
<td>16</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No session timer.</td>
</tr>
</tbody>
</table>
Firewall Traversal Deployment Scenarios

This section provides the firewall traversal scenarios for the Cisco Unified CME line side endpoints.

Firewall Traversal for Soft Phone

For Cisco Unified CME line side, you can deploy an IOS firewall that can be collocated or non-collocated with the Cisco Unified CME.

This is a typical TRP-based trusted IOS firewall traversal deployment between a soft phone and the desk phones. In this scenario, a soft phone like CIPC in the data segment is registered to a Cisco Unified CME. When this soft phone communicates to a desktop IP phone in the voice segment that is registered to the same or different Cisco Unified CME, you can deploy an IOS firewall for the traffic sent between the desktop phone and the soft phone on the Cisco Unified CME line side.

Firewall Traversal for Wireless Phone

In this scenario, the TRP-based trusted IOS firewall traversal is deployed between a wireless phone and desktop phones. A wireless (WiFi) phone like Cisco 792xG is registered to a Cisco Unified CME. When the wireless phone communicates to a wired phone that is registered to the same or different Cisco Unified CME, you can deploy an IOS firewall for the traffic sent between the wired and the wireless phone on the Cisco Unified CME line side.

Firewall Traversal for Teleworker

In this scenario, the teleworker phone is registered to a central or branch office and the Cisco Unified CME communicates to a phone which resides inside the central or branch office. You can deploy an IOS firewall for the traffic sent between the central/branch office and the teleworker phone on the Cisco Unified CME line side.

The teleworker can use the Transport Layer Security (TLS) and Secure Real-Time Protocol (SRTP) for making VoIP calls or establish a Virtual Private Network (VPN) tunnel to the central or branch office for making VoIP calls. In TLS/ SRTP case, the VPN engine/concentrator decrypts the signaling packets and passes the packets to the firewall for inspection. Hence, either a partial SIP ALG or ACL, along with TRP, can be deployed. In VPN case, the firewall will not have the key to decrypt the signaling packets. Hence, only ACL along with TRP can be deployed.

How to Configure Cisco Unified Communications Trusted Firewall Control - Version III

To configure Firewall traversal for Cisco Unified CME SIP line side endpoints, enable the stun-usage under:

- Voice-register pool or voice-register template and apply under the voice register pool for SIP line side

Configuring Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints

Perform these tasks to configure firewall traversal.
### SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool phone-tag
4. voice-class stun-usage tag
5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Device&gt; enable</td>
<td>• Enter your password if prompted</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register pool phone-tag</td>
<td>Enters voice register pool configuration mode to set the phone-specific parameters for an SIP phone.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config)# voice register pool 3</td>
<td>• <em>phone-tag</em>-<em>Unique</em> sequence number that identifies the phone. Range is version and platform-dependent; type ? to display range.</td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class stun-usage tag</td>
<td>Enables voice-class stun-usage on the voice-register pool.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-voice-register-pool)# voice-class stun-usage 1</td>
<td>• This command can also be configured in voice-register-template configuration mode and applied to one or more SIP phones. The voice-register pool configuration has priority over the voice-register-template configuration.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Device(config-voice-register-pool)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Cisco Unified CME SIP Line Side EndPoints**

This section provides the following sample configuration:

```
Device# show run
Building configuration...
!
! Last configuration change at 14:20:02 IST Thu Mar 25 2010 by cisco
! NVRAM config last updated at 15:10:47 IST Wed Mar 24 2010 by cisco
```

---

Finding Feature Information

Configuring Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints

! version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname fidesrst
!
boot-start-marker
boot system tftp://9.13.40.15/kartk/c3845-adventerprisek9_ivs-mz.0_2_0_20091205
boot-end-marker
!
logging buffered 1000000
no logging console
enable secret 5 $1$GbsI$Ah0BLBHwFb4w/Hu7kyhrs1
enable password cisco
!
no aaa new-model
!
no process cpu autoprobe hog
clock timezone IST 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
template 10
!
voice-card 0
dspfarm
dsp services dspfarm
!
voice service voip
notify redirect ip2pots
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
stun
stun flowdata agent-id 1 boot-count 45
stun flowdata shared-secret 7 14141B180F0B7B79772B3A26211C564450
stun flowdata catlife 70 keepalive 30
sip
session transport tcp
registrar server expires max 600 min 60
!
voice class stun-usage 1
stun usage firewall-traversal flowdata
!
voice register global
mode cme
source-address 192.168.0.1 port 5060
max-dn 100
max-pool 100
load 7971 SIP70.8-5-2SR1S
load 7970 SIP70.8-5-2SR1S
load 7961 SIP41.8-5-2SR1S
load 7960-7940 POS3-8-12-00
authenticate realm cisco.com
tftp-path flash:
create profile sync 0221764396482329
!
voice register dn 2
number 999999
pickup-group 333
name 7970-2
mwi
!
voice register dn 3
number 777777
pickup-group 333
name 7970-3
mwi

voice register dn 5
number 2222
name 7960-Camelot1
mwi

voice register dn 6
number 4444
name 7960-Camelot2
mwi

voice register dn 7
number 6666
name 7960-Camelot3
mwi

voice register dn 8
number 8888
call-forward b2bua all 6666
name 7960-Camelot4
mwi

voice register dn 9
number 101010
call-forward b2bua all 1111
name 7960-Camelot5
mwi

voice register dn 10
number 121212
call-forward b2bua noan 6666 timeout 3
name 7960-Camelot6
mwi

voice register dn 11
number 141414
call-forward b2bua busy 1111
name 7960-Camelot7
huntstop channel 1
mwi

voice register dn 50
number 15253545
name callgen-sip1
mwi

voice register dn 51
number 16263646
name callgen-sip2
mwi

voice register template 10
voice-class stun-usage 1
softkeys connected Park Confrn Endcall Hold Trnsfer

voice register pool 2
park reservation-group 1111
id mac 0022.9059.81D9
type 7970
number 1 dn 2
template 10
codec g711ulaw

voice register pool 50
id mac 0011.209F.5D60
type 7960
number 1 dn 50
voice-class stun-usage 1
codec g711ulaw
voice register pool 51
id mac 0011.209F.5D60
type 7960
number 1 dn 51
voice-class stun-usage 1
codec g711ulaw
license udi pid CISCO3845-MB sn FOC12373868
archive
log config
hidekeys
username cisco password 0 cisco
!
redundancy
!
ip ftp username test
ip ftp password test123
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
duplex auto
speed auto
media-type rj45
no keepalive
no cdp enable
!
interface GigabitEthernet0/1
description 192.168.0.1 255.255.255.0
media-type rj45
no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http timeout-policy idle 60 life 600000 requests 100000
!
ip route 0.0.0.0 0.0.0.0 7.9.0.1
ip route 9.13.7.0 255.255.255.0 9.13.7.1
ip route 9.13.7.0 255.255.255.0 9.13.38.1
ip route 9.13.40.0 255.255.255.0 9.13.38.1
ip route 10.104.56.0 255.255.255.0 192.168.0.35
!
arp 10.104.56.54 0024.81b5.3302 ARPA
!
call treatment on
!
voice-port 0/0/0
!
voice-port 0/0/1
!
mgcp fax t38 ecm
!
gateway
timer receive-rtp 1200
!
sip-ua
!
alias exec showrtp show policy-map type inspect zone-pair sessions
!
line con 0
exec-timeout 0 0
login local
line aux 0
line vty 0 4
Configuring Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints

To configure Firewall traversal for Cisco Unified CME SCCP line side endpoints, enable the stun-usage under:

- Ephone or ephone-template and apply under the ephone for SCCP line side

Before You Begin

**Note**

MTP should be enabled under ephones for SCCP CME line side endpoints

### SUMMARY STEPS

1. enable
2. configure terminal
3. ephone phone-tag
4. mtp
5. voice-class stun-usage tag
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 3** ephone **phone-tag** | Enters ephone configuration mode to set phone-specific parameters for an SCCP phone.  
  - **phone-tag** — Unique sequence number that identifies the phone.  
  Range is version and platform-dependent; type `?` to display range. |
| **Example:**  
  Device(config)# ephone 2 |
| **Step 4** mtp | Enables Media Termination Points (MTP) on this ephone. |
| **Example:**  
  Device(config-ephone)# mtp |
| **Step 5** voice-class **stun-usage** **tag** | This command can also be configured in ephone-template configuration mode and applied to one or more SCCP phones. The ephone configuration has priority over the ephone-template configuration. |
| **Example:**  
  Device(config-ephone)# voice-class stun-usage 10000 |
| **Step 6** end | Exits ephone configuration mode and returns to privileged EXEC mode. |
| **Example:**  
  Device(config-ephone)# end |

**Example: Cisco Unified CME SCCP Line Side EndPoints**

This section provides the following sample configuration:

```
Device#show run
Building configuration...
!
! Last configuration change at 14:20:02 IST Thu Mar 25 2010 by cisco
! NVRAM config last updated at 15:10:47 IST Wed Mar 24 2010 by cisco
!
version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname fidesrst
!
boot-start-marker
! boot system tftp://9.13.40.15/kartk/c3845-adventpriskg9_ivs-mz.0_2_0_20091205
boot-end-marker
!
logging buffered 1000000
no logging console
enable secret 5 $1$GbsI$Ah0BLBHfFx4w/Hu7kyhrl
enable password cisco
!
no aaa new-model
!
no process cpu autoprobe hog
clock timezone IST 5
!
dot11 syslog
ip source-route
```
! no ip cef
! no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
! multilink bundle-name authenticated
!
! template 10
!
voice-card 0
dspfarm
dsp services dspfarm
!
voice service voip
  notify redirect ip2pots
  no supplementary-service sip moved-temporarily
  no supplementary-service sip refer
  stun
    stun flowdata agent-id 1 boot-count 45
    stun flowdata shared-secret 7 14141B180F0B7B79772B3A26211C564450
    stun flowdata catlife 70 keepalive 30
  sip
    session transport tcp
    registrar server expires max 600 min 60
  !
voice class stun-usage 1
  stun usage firewall-traversal flowdata
!
!
license udi pid CISCO3845-MB sn FOC12373868
archive
log config
hidekeys
username cisco password 0 cisco
!
redundancy
!
ip ftp username test
ip ftp password test123
!
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
duplex auto
speed auto
media-type rj45
no keepalive
no cdp enable
!
interface GigabitEthernet0/1
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
media-type rj45
no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 7.9.0.1
ip route 9.13.7.0 255.255.255.0 9.13.7.1
ip route 9.13.7.0 255.255.255.0 9.13.38.1
ip route 9.13.40.0 255.255.255.0 9.13.38.1
ip route 10.104.56.0 255.255.255.0 192.168.0.35
!
arp 10.104.56.54 0024.81b5.3302 ARPA
!
control-plane
call treatment on
!
voice-port 0/0/0
!
voice-port 0/0/1
!
mgcp fax t38 ecm
!
ccp local GigabitEthernet0/1
ccp ccm 192.168.0.1 identifier 1 version 7.0
ccp
!
gateway
timer receive-rtp 1200
!
sip-ua
!
telephony-service
sds pfarm units 3
sds pfarm transcode sessions 12
sds pfarm tag 2 HwConference
sds pfarm tag 3 mtp00230471e381
video
srst mode auto-provision all
srst ephone template 1
srst dn line-mode dual
max-ephones 262
max-dn 500
ip source-address 192.168.0.1 port 2000
service directed-pickup gpickup
max-conferences 8 gain -6
call-park system application
moh music-on-hold.au
transfer-system full-consult
create cnf-files version-stamp 7960 Mar 24 2010 15:09:20
!
ephone-template 1
voice-class stun-usage 1
mtp
!
ephone-template 3
voice-class stun-usage 1
!
ephone-dn 1 dual-line
number 1000
name vg1port1
!
ephone-dn 2 dual-line
number 2000
name vg1port2
!
ephone-dn 3 dual-line
number 3000
name vg2port1
!
ephone-dn 4 dual-line
number 4000
name vg2port2
call-forward all 3000
!
ephone-dn 5 dual-line
number 1111
name sccpcamelot1
!
ephone-dn 6 dual-line
number 3333
name sccpcamelot2
!
ephone-dn 7 dual-line
number 717818919
description 717818919
name 717818919

ephone-dn 8 dual-line
  number 6000
  label 6000
  description 6000
  name 6000

ephone-dn 9 dual-line
  number 5000
  label 5000
  description 5000
  name 5000

ephone-dn 10 dual-line

ephone-dn 11 dual-line

ephone-dn 13 dual-line
  number 919886087486
  name blacforestvg0

ephone-dn 14 dual-line
  number 919886087487
  name blacforestvg1

ephone-dn 15 dual-line
  number 919886087488
  name blacforestvg2

ephone-dn 16 dual-line
  number 919886087489
  name blacforestvg3

ephone-dn 41 dual-line
  number 9876
  conference meetme
  preference 1
  no huntstop

ephone-dn 42 dual-line
  number 9876
  conference meetme
  preference 2
  no huntstop

ephone-dn 43 dual-line
  number 9876
  conference meetme
  preference 3
  no huntstop

ephone 1
  voice-class stun-usage 1
  device-security-mode none
  mac-address FCAC.3BAE.0000
  max-calls-per-button 2
  mtp
  type anl
  button 1:1

ephone 2
  voice-class stun-usage 1
  device-security-mode none
  mac-address FCAC.3BAE.0001
  max-calls-per-button 2
  mtp
  type anl
  button 1:2

ephone 3
  voice-class stun-usage 1
  device-security-mode none
Finding Feature Information

Configuring Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints

```
mac-address FCAC.3BAC.0000
max-calls-per-button 2
type anl
button 1:3
!
ephone 4
voice-class stun-usage 1
device-security-mode none
mac-address FCAC.3BAC.0001
max-calls-per-button 2
mtp
type anl
button 1:4
!
ephone 5
voice-class stun-usage 1
device-security-mode none
mac-address 1234.1234.1211
max-calls-per-button 2
mtp
type 7960
button 1:5
!
ephone 6
voice-class stun-usage 1
device-security-mode none
ephone-template 3
max-calls-per-button 2
codec g729r8 dspfarm-assist
mtp
type 7960
button 1:6
!
ephone 7
device-security-mode none
mac-address FCAC.3B79.0001
ephone-template 1
max-calls-per-button 2
type anl
button 1:14
!
ephone 8
device-security-mode none
mac-address 001B.D584.E274
ephone-template 1
button 1:7
!
ephone 9
device-security-mode none
mac-address FCAC.3B7F.0001
ephone-template 1
button 1:8
!
ephone 10
device-security-mode none
mac-address FCAC.3B7F.0000
ephone-template 1
button 1:9
!
ephone 11
device-security-mode none
mac-address FCAC.3B79.0002
ephone-template 1
max-calls-per-button 2
type anl
button 1:15
!
ephone 13
device-security-mode none
mac-address FCAC.3B79.0000
ephone-template 1
max-calls-per-button 2
```
Configuring SIP Session Timers

Configuring SIP Session Timer Globally

Perform these tasks to configure SIP session timer globally.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. min-se\text{string} session-expire\text{string}
6. session refresh
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode and specifies a voice-encapsulation type.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# voice service voip</td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-voi-serv)# sip</td>
</tr>
<tr>
<td><strong>Step 5</strong> min-se <em>string</em> session-expires <em>string</em></td>
<td>Configures the minimum session expires (min-se) and session-expires</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(conf-serv-sip)# min-se 90 session-expires 100</td>
</tr>
<tr>
<td><strong>Step 6</strong> session refresh</td>
<td>Enables SIP session timer globally.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(conf-serv-sip)# session refresh</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Exits SIP configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device (conf-serv-sip)# end</td>
</tr>
</tbody>
</table>

### Example: SIP Session Timer

This section provides the following sample configuration:

Device# show run
show running-config
Building configuration...
Current configuration : 2284 bytes
!
Last configuration change at 13:50:48 IST Sun Mar 14 2010
! NVRAM config last updated at 16:21:46 IST Fri Mar 12 2010
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname CUBE1-Fides3
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
no logging console
!
no aaa new-model
no process cpu autoprobe hog
clock timezone IST 5
!
ip source-route
!
ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
multilink bundle-name authenticated
!
voice service voip
allow-connections sip to sip
sip
min-se 90 session-expires 100
session refresh
!
voice-card 0
!
license udi pid CISCO2821 sn FHK1143P0UK
archive
log config
hidekeys
no memory lite
username cisco privilege 15 secret 5 $1$p0H/$eUuiG4gPjffQFVvUzoDd3/
!
redundancy
!
ip ftp username test
ip ftp password test123
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$INTF-INFO-GE 0/0$
ip address 7.9.9.106 255.255.0.0
duplex auto
speed auto
no cdp enable
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
no cdp enable
!
ip forward-protocol nd
!
ip http server
ip http access-class 23
ip http authentication local
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 7.9.0.1
!
control-plane
!
mgcp fax t38 ecm
!

dial-peer voice 100 voip
huntstop
destination-pattern 1000000000
h2hua
session protocol sipv2
session target ipv4:7.9.9.9
incoming called-number 2000000000
voice-class sip session refresh
codec g711ulaw
!
Perform these tasks to configure SIP session timer at the dial peer level.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dial-peer voice voip
d4. voice-class sip session refresh
d5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td></td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal |
| Example: Device# configure terminal |
| Enters global configuration mode. |

| **Step 3** dial-peer voice voip |
| Example: Device(config)# dial-peer voice 1 voip |
| Enters dial peer configuration mode to define a VoIP dial peer. |
### Purpose

Command or Action | Purpose
--- | ---
Step 4 | **voice-class sip session refresh**

**Example:**

Device(config-dial-peer)# voice-class sip session refresh

Enables SIP session refresh at dial-peer level.

---

Step 5 | **end**

**Example:**

Device(config-ephone)# end

Exits dial-peer configuration mode and returns to privileged EXEC mode.

### Feature Information for Cisco Unified Communications Trusted Firewall Control - Version III

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 39: Feature Information for Cisco Unified Communications Trusted Firewall Control - Version III**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Cisco Unified Communications Trusted Firewall Control - Version III | 15.1(2)T | Cisco Unified Communications Trusted Firewall Control using STUN pushes intelligent services into the network through Trust Relay Point (TRP).

The following commands were introduced or modified: **session refresh**, and **voice-class sip session refresh**.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Cisco Unified Communications Trusted Firewall Control - Version III | Cisco IOS XE Release 3.6S | Cisco Unified Communications Trusted Firewall Control using STUN pushes intelligent services into the network through Trust Relay Point (TRP).  
In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise)  
The following commands were introduced or modified: `session refresh`, and `voice-class sip session refresh`. |
Finding Feature Information

Feature Information for Cisco Unified Communications Trusted Firewall Control - Version III
Domain-Based Routing Support on the Cisco UBE

First Published: June 15, 2011
Last Updated: July 22, 2011

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.

- Feature Information for Domain-Based Routing Support on the Cisco UBE, page 401
- Restrictions for Domain-Based Routing Support on the Cisco UBE, page 402
- Information About Domain-Based Routing Support on the Cisco UBE, page 402
- How to Configure Domain-Based Routing Support on the Cisco UBE, page 403
- Configuration Examples for Domain-Based Routing Support on the Cisco UBE, page 408

Feature Information for Domain-Based Routing Support on the Cisco UBE

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 40: Feature Information for Domain-Based Routing Support on the Cisco UBE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Based Routing Support on the Cisco UBE</td>
<td>15.2(1)T</td>
<td>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.</td>
</tr>
<tr>
<td>Domain Based Routing Support on the Cisco UBE</td>
<td>Cisco IOS XE Release 3.8S</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

### Restrictions for Domain-Based Routing Support on the Cisco UBE

Domain-based routing support is available only for SIP-SIP call flows.

### Information About Domain-Based Routing Support on the Cisco UBE

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.

### How to Configure Domain-Based Routing Support on the Cisco UBE

#### Configuring 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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enter your password if prompted.</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Enters voice service configuration mode.</td>
<td>voice service voip</td>
</tr>
<tr>
<td>Enters voice service SIP configuration mode.</td>
<td>sip</td>
</tr>
<tr>
<td>Routes calls based on the URL.</td>
<td>call-route url</td>
</tr>
<tr>
<td>Exits the current mode.</td>
<td>exit</td>
</tr>
</tbody>
</table>

## Configuring 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 dial-peer voice dial-peer tag voip</td>
<td>Enter dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 voice-class sip call-route url</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)#</td>
<td></td>
</tr>
<tr>
<td>Example: Routes calls based on the URL</td>
<td></td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Device(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying and Troubleshooting Domain-Based Routing Support on the Cisco UBE

#### SUMMARY STEPS

1. enable
2. debug ccsip all
3. debug voip dialpeer inout

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td></td>
</tr>
</tbody>
</table>

IOS XE Release 3S
Enables privileged EXEC mode.

**Example:**

```
Device> enable
```

**Step 2**

**debug ccsip all**

Enables all SIP-related debugging.

**Example:**

```
Device# debug ccsip all
```

```
Received:
Via: SIP/2.0/UDP [2208:1:1:1:1:1:1:1115]:5060;branch=z9hG4bK83AE3
Remote-Party-ID: <sip:2222222222@2208:1:1:1:1:1:1:1115>;party=calling;screen=no;privacy=off
Date: Tue, 01 Mar 2011 08:49:48 GMT
Supported: 100rel,timer,resource-priority,replaces
Require: sdp-anat
Min-SE: 1800
Cisco-Guid: 2948477781-1125585376-2396638033-3925258737
User-Agent: Cisco-SIPGateway/IOS-15.1(3.14.2)P1A16
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, P-RACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1298969388
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 495
v=0
s=SIP Call
a=group:ANAT 1 2
m=audio 17836 RTP/AVP 0 101 19
a=IN IP6 2208:1:1:1:1:1:1:1115
a=mid:1
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtmp:101 0-16
a=rtmp:19 CN/8000
a=ptime:20
m=audio 18938 RTP/AVP 0 101 19
a=IN IP4 9.45.36.111
a=mid:2
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtmp:101 0-16
a=rtmp:19 CN/8000
a=ptime:20
```

```
Received:
INVITE sip:2222222222@2208:1:1:1:1:1:1117]:5060 SIP/2.0
Via: SIP/2.0/UDP [2208:1:1:1:1:1:1:1116]:5060;branch=z9hG4bK38ACE
Date: Thu, 10 Feb 2011 12:15:08 GMT
Call-ID: 5DEDB77e-ADCl1208-808B770-8FCACF34@2208:1:1:1:1:1:1:1117
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE: 1800
Cisco-Guid: 1432849350-0876876256-2424621905-3925258737
```

Step 3

des voip dialpeer inout

The debug ccsip all and debug voip dialpeer inout commands can be entered in any order and any of the commands can be used for debugging depending on the requirement.

Example:

Displays information about the voice dial peers

Device> debug voip dialpeer inout

voip dialpeer inout debugging is on

The following event shows the calling and called numbers:

Example:

*May 1 19:32:11.731: //1-6372E2598012/DPM/dpAssociateIncomingPeerCore:
  Calling Number=408555111, 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

The following event shows the incoming dial peer:

Example:

*May 1 19:32:11.731: //1-6372E2598012/DPM/dpAssociateIncomingPeerCore:
  Result=Success after DP_MATCH_INCOMING_DNIS; Incoming Dial-peer=100
*May 1 19:32:11.731: //1-6372E2598012/DPM/dpAssociateIncomingPeerCore:
  Calling Number=408555111, 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 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 after DP_MATCH_DEST
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 Support on the Cisco UBE**

**Example Configuring Domain-Based Routing Support on the Cisco UBE**

The following example shows how to enable domain-based routing support on the Cisco UBE:

```
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 36

URI-Based Dialing Enhancements

The URI-Based Dialing Enhancements feature describes the enhancements made to Uniform Resource Identifier (URI)-based dialing on Cisco Unified Border Element (Cisco UBE) for Session Initiation Protocol (SIP) calls. The URI-Based Dialing Enhancements feature includes support for call routing on Cisco UBE when the user part of the incoming Request-URI is non-E164 (for example, INVITE sip:user@abc.com).

• Finding Feature Information, page 409
• Information About URI-Based Dialing Enhancements, page 409
• How to Configure URI-Based Dialing Enhancements, page 413
• Configuration Examples for URI-Based Dialing Enhancements, page 421
• Additional References for URI-Based Dialing Enhancements, page 423
• Feature Information for URI-Based Dialing Enhancements, page 423

Finding Feature Information

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

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

Information About URI-Based Dialing Enhancements

Cisco Unified Communications Manager (CUCM) 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. A directory URI is a string of characters that can be used to identify a directory number. If that directory number is assigned to a phone, CUCM 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 primary use of URI-based dialing is peer-to-peer calling between enterprises using complete URI addresses (that is, ‘username@host’). The host part of the URI identifies the destination to which the call should be routed. In earlier Cisco Unified Border Element (Cisco UBE) URI routing, the URI was replaced in the SIP header with the destination server IP address. Then routing of calls was based on the following restrictions:

- The user part of the incoming Request-URI must be an E164 number.
- The outgoing Request-URI is always set to the session target information of the outbound dial peer.

The URI-Based Dialing Enhancements feature extends support for Cisco UBE URI-based routing of calls. With these enhancements Cisco UBE supports:

- URI-based routing when the user part of the incoming Request-URI is non-E164 (for example, INVITE sip:user@abc.com).
- URI-based 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-based 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.

### Call Flows for URI-Based Dialing Enhancements

Case 1: URI dialing with username being E164 or non-E164 number and Request-URI host copied from the inbound leg.

![Call Flow Diagram](image)

Case 2: Incoming Request-URI does not contain user part. The To: header information is also copied from the peer leg when the `requri-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.
How to Configure URI-Based Dialing Enhancements

Configuring Pass Through of SIP URI Headers

Perform these 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, Cisco Unified Border Element (Cisco UBE) 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-based Dialing Enhancements" section.
Configuring Pass Through 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>voice service voip</td>
<td>Specifies VoIP encapsulation and enters voice service configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>sip</td>
<td>Enters the Session Initiation Protocol (SIP) configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>requri-passing</td>
<td>Enables pass through of the host part of the Request-URI and To SIP headers. By default, Cisco UBE sets the host part of the URI to the value configured under the session target of the outbound dial peer.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(conf-serv-sip)# requri-passing</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(conf-serv-sip)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Pass Though 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>voice class uri tag sip</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# voice class uri mydesturi sip</code></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Creates a voice class for matching dial peers to a Session Initiation Protocol (SIP) and enters voice URI class configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>host hostname-pattern</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-voice-uri-class)# host example.com</code></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Matches a call based on the host field in a SIP Uniform Resource Identifier (URI).</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>exit</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config-voice-uri-class)# exit</code></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Exits voice URI class configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>dial-peer voice tag voip</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# dial-peer voice 22 voip</code></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Defines a VoIP dial peer and enters dial peer configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>7</td>
<td>session protocol sipv2</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-dial-peer)# session protocol sipv2</td>
</tr>
<tr>
<td>8</td>
<td>destination uri tag</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# destination uri mydesturi</td>
</tr>
<tr>
<td>9</td>
<td>session target ipv4:ip-address</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-dial-peer)# session target ipv4:10.1.1.2</td>
</tr>
<tr>
<td>10</td>
<td>voice-class sip requiri-passing [system]</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-dial-peer)# voice-class sip requiri-passing system</td>
</tr>
<tr>
<td>11</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-dial-peer)# end</td>
</tr>
</tbody>
</table>

**Configuring Pass Through of 302 Contact Header**

**Configuring 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
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable           | Enables privileged EXEC mode.  
Example:  
Device> enable |  
• Enter your password if prompted. |
| 2    | configure terminal | Enters global configuration mode.  
Example:  
Device# configure terminal |
| 3    | voice service voip | Specifies VoIP encapsulation and enters voice service configuration mode.  
Example:  
Device(config)# voice service voip |
| 4    | sip              | Enters voice service SIP configuration mode.  
Example:  
Device(conf-voi-serv)# sip |
| 5    | contact-passing  | Enables pass through of the contact header from one leg to the other leg in 302 pass through scenario.  
Example:  
Router(conf-serv-sip)# contact-passing |
| 6    | end              | Ends the current configuration session and returns to privileged EXEC mode.  
Example:  
Router(conf-serv-sip)# end |
Configuring 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>voice class uri destination-tag sip</td>
<td>Creates a voice class for matching dial peers to a Session Initiation Protocol (SIP) and enters voice URI class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# voice class uri mydesturi sip</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>user-id id-tag</td>
<td>Matches a call based on the User ID portion of the Uniform Resource Identifier (URI).</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-voice-uri-class)# user-id 5678</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
<td>Exits voice URI class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-voice-uri-class)# exit</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>6</td>
<td><code>voice service voip</code></td>
<td>Specifies Voice over IP (VoIP) as the voice encapsulation type and enters voice service configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config)# voice service voip</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>allow-connections sip to sip</code></td>
<td>Allows connections between SIP endpoints in a VoIP network.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(conf-voi-serv)# allow-connections sip to sip</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>dial-peer voice tag voip</code></td>
<td>Defines a VoIP dial peer and enters dial peer configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config)# dial-peer voice 200 voip</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>session protocol sipv2</code></td>
<td>Specifies a session protocol for calls between local and remote routers using the Internet Engineering Task Force (IETF) SIP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-dial-peer)# session protocol sipv2</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>destination uri destination-tag</code></td>
<td>Specifies the voice class used to match a dial peer to the destination URI of an outgoing call.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-dial-peer)# destination uri mydesturi</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>voice-class sip contact-passing</code></td>
<td>Enables pass through of the contact header from one leg to the other leg in 302 pass through scenario.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-dial-peer)# voice-class sip contact-passing</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>end</code></td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Device(config-dial-peer)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Deriving of 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
<p>| <strong>Example:</strong> Device&gt; enable |
| <strong>Step 2</strong> configure terminal | Enters global configuration mode. |
| <strong>Example:</strong> Device# configure terminal |
| <strong>Step 3</strong> voice class uri destination-tag sip | Creates or modifies a voice class for matching dial peers to a Session Initiation Protocol (SIP) or telephone (TEL) Uniform Resource Identifier (URI) and enters voice URI class configuration mode. |
| <strong>Example:</strong> Device(config)# voice class uri mydesturi sip |
| <strong>Step 4</strong> host hostname-pattern | Matches a call based on the host field in a SIP URI. |
| <strong>Example:</strong> Device(config-voice-uri-class)# host destination.com |
| <strong>Step 5</strong> exit | Exits voice URI class configuration mode. |
| <strong>Example:</strong> Device(config-voice-uri-class)# exit |
| <strong>Step 6</strong> dial-peer voice tag voip | Defines a VoIP dial peer and enters dial peer configuration mode. |
| <strong>Example:</strong> Device(config)# dial-peer voice 25 voip |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies a session protocol for calls between local and remote routers using the Internet Engineering Task Force (IETF) SIP.</td>
</tr>
<tr>
<td>session protocol sipv2</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# session protocol sipv2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Specifies the voice class used to match a dial peer to the destination URI of an outgoing call.</td>
</tr>
<tr>
<td>destination uri destination-tag</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# destination uri mydesturi</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Derives session target from incoming URI.</td>
</tr>
<tr>
<td>session target sip-uri</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# session target sip-uri</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Exits dial peer voice configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Creates or modifies a voice class for matching dial peers to a SIP or TEL URI and enters voice URI class configuration mode.</td>
</tr>
<tr>
<td>voice class uri source-tag sip</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# voice class uri mysourceuri sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Matches a call based on the host field in a SIP URI.</td>
</tr>
<tr>
<td>host hostname-pattern</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-voice-uri-class)# host abc.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-voice-uri-class)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuration Examples for URI-Based Dialing Enhancements

### 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
```
Example: Configuring Pass Though 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 requri-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(config-voi-serv)# sip
Device(config-serv-sip)# contact-passing
Device(config-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(config-voi-serv)# allow-connections sip to sip
Device(config-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

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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>SIP configuration tasks</td>
<td>SIP Configuration Guide, Cisco IOS Release 15M&amp;T</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

Feature Information for URI-Based Dialing Enhancements

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 URI-Based Dialing Enhancements

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>URI-Based Dialing Enhancements</td>
<td>Cisco IOS XE Release 3.11S</td>
<td>The URI-Based Dialing Enhancements feature includes support for call routing on Cisco UBE when the user-part of the incoming Request-URI is non-E164 (for example, INVITE sip:<a href="mailto:user@abc.com">user@abc.com</a>). The following commands were introduced or modified: contact-passing, requiri-passing, session target sip-uri and voice-class sip requiri-passing</td>
</tr>
</tbody>
</table>
Additional References

The following sections provide references related to the CUBE Configuration Guide.

- Related References, page 425
- Standards, page 426
- MIBs, page 427
- RFCs, page 427
- Technical Assistance, page 429

Related References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Navigator</td>
<td>For information about platforms supported, and Cisco IOS software image support, search by Feature Name listed in Feature Information Table in <a href="http://www.cisco.com/go/cfn">www.cisco.com/go/cfn</a></td>
</tr>
<tr>
<td>Bug Search Tool Kit</td>
<td>For information about latest caveats and feature information, see Bug Search Tool</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS Voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
</tbody>
</table>
### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITU-T G.711</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-PROCESS MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-MEMORY-POOL-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-SIP-UA-MIB</td>
<td></td>
</tr>
<tr>
<td>• DIAL-CONTROL-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-VOICE-DIAL-CONTROL-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-DSP-MGMT-MIB</td>
<td></td>
</tr>
<tr>
<td>• IF-MIB</td>
<td></td>
</tr>
<tr>
<td>• IP-TAP-MIB</td>
<td></td>
</tr>
<tr>
<td>• TAP2-MIB</td>
<td></td>
</tr>
<tr>
<td>• USER-_CONNECTION-TAP-MIB</td>
<td></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1889</td>
<td>RTP: A Transport Protocol for Real-Time Applications</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>RFC 2132</td>
<td>DHCP Options and BOOTP Vendor Extensions</td>
</tr>
<tr>
<td>RFC 2198</td>
<td>RTP Payload for Redundant Audio Data</td>
</tr>
<tr>
<td>RFC 2327</td>
<td>SDP: Session Description Protocol</td>
</tr>
<tr>
<td>RFC 2543</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
<tr>
<td>RFC 2543-bis-04</td>
<td>SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt</td>
</tr>
<tr>
<td>RFC 2782</td>
<td>A DNS RR for Specifying the Location of Services (DNS SRV)</td>
</tr>
<tr>
<td>RFC 2806</td>
<td>URLs for Telephone Calls</td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>RFC 2833</td>
<td>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</td>
</tr>
<tr>
<td>RFC 3203</td>
<td>DHCP reconfigure extension</td>
</tr>
<tr>
<td>RFC 3261</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
<tr>
<td>RFC 3262</td>
<td>Reliability of Provisional Responses in Session Initiation Protocol (SIP)</td>
</tr>
<tr>
<td>RFC 3323</td>
<td>A Privacy Mechanism for the Session Initiation Protocol (SIP)</td>
</tr>
<tr>
<td>RFC 3325</td>
<td>Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks</td>
</tr>
<tr>
<td>RFC 3515</td>
<td>The Session Initiation Protocol (SIP) Refer Method</td>
</tr>
<tr>
<td>RFC 3361</td>
<td>Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers</td>
</tr>
<tr>
<td>RFC 3455</td>
<td>Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)</td>
</tr>
<tr>
<td>RFC 3608</td>
<td>Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration</td>
</tr>
<tr>
<td>RFC 3711</td>
<td>The Secure Real-time Transport Protocol (SRTP)</td>
</tr>
<tr>
<td>RFC 3925</td>
<td>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</td>
</tr>
</tbody>
</table>
## Technical Assistance

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

- AMR-NB — Adaptive Multi Rate codec - Narrow Band.
- Allow header — Lists the set of methods supported by the UA generating the message.
- bind — In SIP, configuring the source address for signaling and media packets to the IP address of a specific interface.
- call — In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call identifier. A point-to-point IP telephony conversation maps into a single SIP call.
- call leg — A logical connection between the router and another endpoint.
- CLI — command-line interface.
- Content-Type header — Specifies the media type of the message body.
- CSeq header — Serves as a way to identify and order transactions. It consists of a sequence number and a method. It uniquely identifies transactions and differentiates between new requests and request retransmissions.
- delta — An incremental value. In this case, the delta is the difference between the current time and the time when the response occurred.
- dial peer — An addressable call endpoint.
- DNS — Domain Name System. Used to translate H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.
- DNS SRV — Domain Name System Server. Used to locate servers for a given service.
- DSP — Digital Signal Processor.
- DTMF — dual-tone multifrequency. Use of two simultaneous voice-band tones for dialing (such as touch-tone).
- EFXS — IP phone virtual voice ports.
- FQDN — fully qualified domain name. Complete domain name including the host portion; for example, serverA.companyA.com.
FXS — analog telephone voice ports.

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

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

iLBC — internet Low Bitrate Codec.

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

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

ISDN — Integrated Services Digital Network.

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

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

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

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

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

PER — Packed Encoding Rule.

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

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

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

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

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

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

RFC — Request For Comments.

RTP — Real-Time Transport Protocol (RFC 1889)

SCCP — Skinny Client Control Protocol.

SDP — Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.
session — A SIP session is a set of multimedia senders and receivers and the data streams flowing between the senders and receivers. A SIP multimedia conference is an example of a session. The called party can be invited several times by different calls to the same session.

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

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

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

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

SPI — service provider interface.

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

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

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

TDM — time-division multiplexing.

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

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

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

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

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

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

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

VFC — Voice Feature Card.

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