CONTENTS

Preface i
Audience ii-1
Conventions ii-1
Obtain Documentation and Submit a Service Request ii-2

Cisco Unified Survivable Remote Site Telephony Feature Roadmap iii-iii

Contents iii-iii
Documentation Organization iii-iv
Feature Roadmap iii-v
Information About New Features in Cisco Unified SRST iii-xi
New Features for Unified SRST Version 12.6 iii-xi
New Features for Unified SRST Version 12.3 iii-xi
New Features for Unified SRST Version 12.2 iii-xii
New Features for Unified SRST Version 12.1 iii-xii
New Feature for Unified SRST Version 12.0 iii-xii
New Features for Cisco Unified SRST Version 11.0 iii-xii
New Features for Cisco Unified SRST Version 10.5 iii-xii
  Support for Cisco Unified DX650 SIP IP Phones iii-xiii
  Support for Cisco Unified 78xx SIP IP Phones iii-xiii
New Features in Cisco Unified SRST Version 10.0 iii-xiii
  Cisco Jabber for Windows iii-xiii
  Version Negotiation for Cisco Unified SIP IP Phones iii-xiv
New Features in Cisco Unified SRST Version 9.5 iii-xiv
  After-hour Pattern Blocking Support for Regular Expressions iii-xiv
  Call Park Recall Enhancement iii-xv
  Park Monitor iii-xvi
  Display Support for Name of Called Voice Hunt Groups iii-xvi
  Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups iii-xvii
  Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones iii-xviii
  transfer-pattern iii-xviii
  Backward Compatibility iii-xix
  Dial Plans iii-xix
  transfer max-length iii-xix
  transfer-pattern blocked iii-xix
New Features in Cisco SRST Version 3.2  iii-xxxiii
   Enhancement to the alias Command iii-xxxiii
   Enhancement to the cor Command iii-xxxiv
   Enhancement to the pickup Command iii-xxxiv
   Enhancement to the user-locale Command iii-xxxiv
   Increased the Number of Cisco Unified IP Phones Supported on the Cisco 3845 iii-xxxiv
   MOH Live-Feed Support iii-xxxiv
   No Timeout for Call Preservation iii-xxxv
   RFC 2833 DTMF Relay Support iii-xxxv
   Translation Profile Support iii-xxxv
New Features in Cisco SRST Version 3.1 iii-xxxv
   Cisco Unified IP Phone 7920 Support iii-xxxvi
   Cisco Unified IP Phone 7936 Support iii-xxxvi
New Features in Cisco SRST Version 3.0 iii-xxxvi
   Additional Language Options for IP Phone Display iii-xxxvi
   Consultative Call Transfer and Forward Using H.450.2 and H.450.3 for SCCP Phones iii-xxxvii
   Customized System Message for Cisco Unified IP Phones iii-xxxvii
   Dual-Line Mode iii-xxxvii
   E1 R2 Signaling Support iii-xxxviii
   European Date Formats iii-xxxix
   Huntstop for Dual-Line Mode iii-xxxix
   Music-on-Hold for Multicast from Flash Files iii-xxxix
   Ringing Timeout Default iii-xxxix
   Secondary Dial Tone iii-xxxix
   Enhancement to the show ephone Command iii-xl
   System Log Messages for Phone Registrations iii-xl
   Three-Party G.711 Ad Hoc Conferencing iii-xl
   Support for Cisco VG248 Analog Phone Gateway 1.2(1) and Higher Versions iii-xl
New Features in Cisco SRST Version 2.1 iii-xl
   Additional Language Options for IP Phone Display iii-xl
   Cisco SRST Aggregation iii-xl
   Cisco ATA 186 and ATA 188 Support iii-xl
   Cisco Unified IP Phone 7902G Support iii-xl
   Cisco Unified IP Phone 7905G Support iii-xl
   Cisco Unified IP Phone 7912G Support iii-xl
   Cisco Unified IP Phone Expansion Module 7914 Support iii-xl
   Enhancement to the dialplan-pattern Command iii-xl
New Features in Cisco SRST Version 2.02 iii-xl
   Cisco Unified IP Phone Conference Station 7935 Support iii-xl
Examples 2-91
Example for Configuring Unified SIP SRST on Cisco 4000 Series Integrated Services Routers 2-91
Example for Configuring Voice Hunt Groups in Unified SIP SRST 2-91
Examples for Configuring IPv6 Pools for SIP IP Phones 2-92
Example for Configuring Call Blocking Based on Time of Day, Day of Week, or Date 2-93
Example for Configuring Music On Hold for Unified SIP SRST 2-93
Example for Configuring SIP-to-SIP Call Forwarding on Unified SRST 2-93
Example for Configuring Idle Prompt Status for SIP Phones 2-93
Example for Disabling SIP Supplementary Services for Call Forward and Call Transfer 2-94

Cisco Unified Enhanced Survivable Remote Site Telephony 3-95

Contents 3-95
Migration from Unified SRST Manager to Unified E-SRST 3-95
Benefits of Unified-ESRST 3-96
Toll Fraud Prevention for SIP Line Side on Unified E-SRST 3-96
Unified E-SRST with Support for Voice Hunt Group 3-96
Support for B-ACD in Unified E-SRST 3-97
Recommendations for Configuring Voice Hunt Group on Unified E-SRST 3-97
Restrictions for Unified E-SRST, Release 12.2 3-98
SIP: Configure Unified E-SRST 3-98
Restrictions 3-99
Enable the E-SRST Mode 3-100
Configure SIP shared-line 3-100
Configure BLF 3-101
Enable a SIP Directory Number to be Watched 3-101
Enable BLF on a Voice Register Pool 3-101
Configure Unified E-SRST 3-103
DETAILED STEPS 3-104
Configure Voice Hunt Groups on Unified E-SRST 3-107
DETAILED STEPS 3-108
Example for configuring Unified E-SRST with Voice Hunt Group Enhancements 3-109
Example for Configuring B-ACD with Unified E-SRST 3-110
Example for Configuring Shared Line with Voice Hunt Group on Unified E-SRST 3-111
SCCP: Configure Unified E-SRST 3-114
Prerequisites 3-114
Configure Mixed Shared Lines with SCCP Phones 3-118
Configure BLF for SCCP Phones 3-119
Enable an SCCP Directory Number to be Watched 3-119
Enable BLF on an Ephone 3-120
Configure Digest Credentials On Unified Communications Manager 3-120
## Contents

- **Configure Digest Credentials on Unified E-SRST for SIP** 3-120
- **Configure Digest Credentials on Unified E-SRST for SCCP** 3-121
- **Unified E-SRST Scale Support** 3-121
- **Where to Go Next** 3-122

### Setting Up the Network 4-123

- **Contents** 4-123
  - **Information About Setting Up the Network** 4-124
  - **How to Set Up the Network** 4-124
    - **Enabling IP Routing** 4-124
    - **Enabling Cisco Unified SRST on an MGCP Gateway** 4-124
      - Configuring Cisco Unified SRST on an MGCP Gateway Prior to Cisco IOS Release 12.3(14)T 4-125
      - Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later Releases 4-126
      - **Restrictions** 4-126
      - Configuration Example of Enabling SRST on a MGCP Gateway using Cisco IOS Release 12.3(14)T 4-128
    - **Configuring DHCP for Cisco Unified SRST Phones** 4-130
      - Defining a Single DHCP IP Address Pool 4-130
      - Defining a Separate DHCP IP Address Pool for Each Cisco Unified IP Phone 4-131
      - **Defining the DHCP Relay Server** 4-132
      - **Specifying Keepalive Intervals** 4-133
    - **Examples** 4-134
  - **Where to Go Next** 4-134

### Cisco Unified SIP SRST 4.1 5-135

- **Contents** 5-135
  - **Prerequisites for Cisco Unified SIP SRST 4.1** 5-135
  - **Restrictions for Cisco Unified SIP SRST 4.1** 5-136
  - **Information About Cisco Unified SIP SRST 4.1** 5-136
    - **Out-of-Dialog REFER** 5-136
    - **Digit Collection on SIP Phones** 5-137
      - **KPML Digit Collection** 5-137
      - **SIP Dial Plans** 5-137
    - **Caller ID Display** 5-138
    - **Disabling SIP Supplementary Services for Call Forward and Call Transfer** 5-138
    - **Idle Prompt Status** 5-138
    - **Enhanced 911 Services** 5-138
  - **How to Configure Cisco Unified SIP SRST 4.1 Features** 5-139
Enabling KPML for SIP Phones  5-139  
Restrictions  5-139  
What to Do Next  5-140  
Disabling SIP Supplementary Services for Call Forward and Call Transfer  5-141  
Configuring Idle Prompt Status for SIP Phones  5-142  
Prerequisites  5-142  
Where to Go Next  5-143

Setting Up Cisco Unified IP Phones using SCCP  6-145  
Contents  6-145  
Information About Setting Up Cisco Unified IP Phones  6-145  
How to Set Up Cisco Unified IP Phones  6-146  
Configuring Cisco Unified SRST to Support Phone Functions  6-146  
Configuring Cisco Unified 8941 and 8945 SCCP IP Phones  6-148  
Verifying That Cisco Unified SRST Is Enabled  6-149  
Configuring IP Phone Clock, Date, and Time Formats  6-150  
Example  6-151  
Configuring IP Phone Language Display  6-152  
Examples  6-153  
Configuring Customized System Messages for Cisco Unified IP Phones  6-154  
Examples  6-155  
Configuring a Secondary Dial Tone  6-155  
Examples  6-155  
Configuring Dual-Line Phones  6-156  
Examples  6-157  
Configuring Eight Calls per Button (Octo-Line)  6-158  
Prerequisites  6-158  
Restrictions  6-158  
Examples  6-160  
Configuring the Maximum Number of Calls  6-160  
Prerequisites  6-160  
Troubleshooting  6-162  
How to Set Up Cisco IP Communicator for Cisco Unified SRST  6-162  
Prerequisites  6-162  
Verifying Cisco IP Communicator  6-163  
Troubleshooting Cisco IP Communicator  6-163  
Where to Go Next  6-163

Setting Up Cisco Unified IP Phones using SIP  7-165  
Contents  7-165
Enabling Digit Translation Rules 8-199
Examples 8-200
Enabling Translation Profiles 8-200
Examples 8-203
Verifying Translation Profiles 8-203
Configuring Dial-Peer and Channel Hunting 8-204
Examples 8-205
Configuring Busy Timeout 8-205
Examples 8-206
Configuring the Ringing Timeout Default 8-206
Examples 8-207
Configuring Outgoing Calls 8-207
Configuring Local and Remote Call Transfer 8-207
Examples 8-208
Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0 8-208
Examples 8-211
Enabling Analog Transfer Using Hookflash and the H.450.2 Standard with Cisco SRST 3.0 or Earlier 8-212
Examples 8-216
Configuring Trunk Access Codes 8-216
Examples 8-217
Configuring Interdigit Timeout Values 8-217
Examples 8-218
Configuring Class of Restriction 8-218
Examples 8-220
Call Blocking (Toll Bar) Based on Time of Day and Day of Week or Date 8-222
Examples 8-223
How to Configure Cisco Unified SIP SRST 8-224
Configuring SIP Phone Features 8-224
Configuring SIP-to-SIP Call Forwarding 8-226
Configuring Call Blocking Based on Time of Day, Day of Week, or Date 8-228
Examples 8-231
Verification 8-231
SIP Call Hold and Resume 8-232
Examples 8-232
How to Configure Optional Features 8-234
Enabling Three-Party G.711 Ad Hoc Conferencing 8-234
Examples 8-235
Defining XML API Schema 8-236
Configuration Examples for Call Handling 8-236
Example: Monitoring the Status of Key Expansion Modules 8-236
Example: Configuring Voice Hunt Groups in Cisco Unified SIP SRST 8-237
Where to Go Next 8-237

Configuring Secure SRST for SCCP and SIP 9-239

Contents 9-239
Prerequisites for Configuring Secure SRST 9-239
Restrictions for Configuring Secure SRST 9-240
Information About Configuring Secure SRST 9-242
Benefits of Secure SRST 9-242
Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router 9-242
Secure Music On Hold for Unified Secure SRST (SIP) 9-243
Secure SCCP SRST on Cisco 4000 Series Integrated Services Router 9-243
Secure SCCP SRST for Analog Voice Gateways 9-243
Secure Music On Hold for Secure Unified SRST (SCCP) 9-244
Three-way Software Conferencing for Secure SCCP, Unified SRST Release 12.3 9-244
Feature Support for Secure SRST (SCCP), Unified SRST Release 12.3 9-246
Cisco IP Phones Clear-Text Fallback During Non-Secure SRST 9-246
Signaling Security on Unified SRST - TLS 9-246
SRST Routers and the TLS Protocol 9-247
TLS Cipher Support for Secure SRST 12.6 and Later Releases 9-248
TLS_DHE_RSA_WITH_AES_128_CBC_SHA1 9-249
Certificates Operation on Secure SRST 9-249
Certificates Transport from CUCM to Secure SRST 9-251
Media Security on Unified SRST - SRTP 9-251
Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone 9-252
Secure SRST Authentication and Encryption 9-253
How to Configure Secure Unified SRST 9-254
Preparing the Cisco Unified SRST Router for Secure Communication 9-255
Configuring a Certificate Authority Server on a Cisco IOS Certificate Server 9-255
Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server 9-257
Disabling Automatic Certificate Enrollment 9-261
What to Do Next 9-261
Verifying Certificate Enrollment 9-262
Enabling Credentials Service on the Secure Cisco Unified SRST Router 9-264
Troubleshooting Credential Settings 9-266
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importing Phone Certificate Files in PEM Format to the Secure SRST Router</td>
<td>9-266</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager 4.X.X and Earlier Versions</td>
<td>9-267</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager 5.0 and Later Versions</td>
<td>9-267</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager 6.0 and Later Versions</td>
<td>9-268</td>
</tr>
<tr>
<td>Authenticating the Imported Certificates on the Cisco Unified SRST Router</td>
<td>9-268</td>
</tr>
<tr>
<td>What to Do Next</td>
<td>9-269</td>
</tr>
<tr>
<td>Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router</td>
<td>9-274</td>
</tr>
<tr>
<td>Adding an SRST Reference to Cisco Unified Communications Manager</td>
<td>9-274</td>
</tr>
<tr>
<td>Configuring SRST Fallback on Cisco Unified Communications Manager</td>
<td>9-275</td>
</tr>
<tr>
<td>Configuring CAPF on Cisco Unified Communications Manager</td>
<td>9-277</td>
</tr>
<tr>
<td>Enabling SRST Mode on the Secure Cisco Unified SRST Router</td>
<td>9-277</td>
</tr>
<tr>
<td>Configuring Secure SCCP SRST</td>
<td>9-279</td>
</tr>
<tr>
<td>Prerequisites for Configuring Secure SCCP SRST</td>
<td>9-279</td>
</tr>
<tr>
<td>Restrictions for Configuring Secure SCCP SRST</td>
<td>9-279</td>
</tr>
<tr>
<td>Verifying Phone Status and Registrations</td>
<td>9-280</td>
</tr>
<tr>
<td>Configuration Examples for Secure SCCP SRST</td>
<td>9-287</td>
</tr>
<tr>
<td>Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST</td>
<td>9-293</td>
</tr>
<tr>
<td>Prerequisites for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST</td>
<td>9-293</td>
</tr>
<tr>
<td>Restrictions for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST</td>
<td>9-293</td>
</tr>
<tr>
<td>Information About Cisco Unified SIP SRST Support of Secure SIP Signaling and SRTP Media</td>
<td>9-294</td>
</tr>
<tr>
<td>Configuring Cisco Unified Communications Manager</td>
<td>9-294</td>
</tr>
<tr>
<td>Configuring Phones</td>
<td>9-295</td>
</tr>
<tr>
<td>Configuring SIP options for Secure SIP SRST</td>
<td>9-296</td>
</tr>
<tr>
<td>Configuring SIP SRST Security Policy</td>
<td>9-297</td>
</tr>
<tr>
<td>Configuring SIP User Agent for Secure SIP SRST</td>
<td>9-298</td>
</tr>
<tr>
<td>Configuration Example for Cisco Unified SIP SRST</td>
<td>9-302</td>
</tr>
<tr>
<td>Additional References</td>
<td>9-308</td>
</tr>
<tr>
<td>Related Documents</td>
<td>9-309</td>
</tr>
<tr>
<td>Standards</td>
<td>9-309</td>
</tr>
<tr>
<td>MIBs</td>
<td>9-309</td>
</tr>
<tr>
<td>RFCs</td>
<td>9-309</td>
</tr>
<tr>
<td>Technical Assistance</td>
<td>9-310</td>
</tr>
<tr>
<td>Command Reference</td>
<td>9-310</td>
</tr>
<tr>
<td>Feature Information for Secure SCCP and SIP SRST</td>
<td>9-311</td>
</tr>
</tbody>
</table>
Where to Go Next

**Configuring SIP Trunking on Unified SRST**

Contents

Unified SRST and Unified Border Element Co-location

Configuration Recommendations for Unified SRST and Unified Border Element Co-location

Restrictions

Examples

Feature Information for Configuring SIP Trunking on Unified SRST

**Integrating Voicemail with Cisco Unified SRST**

Contents

Information About Integrating Voicemail with Cisco Unified SRST

How to Integrate Voicemail with Cisco Unified SCCP and SIP SRST

Configuring Direct Access to Voicemail

Examples

Configuring Message Buttons

Examples

Redirecting to Cisco Unified Communications Manager Gateway

Configuring Call Forwarding to Voicemail

Call Routing Instructions Using DTMF Digit Patterns

Prerequisites

Examples

Configuring Message Waiting Indication (Cisco Unified SRST Routers)

Configuring Message Waiting Indication (SIP Phones in SRST Mode)

Configuration Examples for Unified SRST

Configuring Local Voicemail System (FXO and FXS): Example

Configuring Central Location Voicemail System (FXO and FXS): Example

Configuring Voicemail Access over FXO and FXS: Example

Configuring Voicemail Access over BRI and PRI: Example

Message Waiting Indication for SIP SRST: Example

How to Configure DTMF Relay for SIP Applications and Voicemail

DTMF Relay Using SIP RFC 2833

Troubleshooting Tips

DTMF Relay Using SIP Notify (Nonstandard)

Troubleshooting Tips

Where to Go Next
Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource  B-11

Contents  B-11

Prerequisites for Using Cisco Unified SRST Gateways as a Multicast MOH Resource  B-12
Restrictions for Using Cisco Unified SRST Gateways as a Multicast MOH Resource  B-12
Information About Using Cisco Unified SRST Gateways as a Multicast MOH Resource  B-13
  Cisco Unified SRST Gateways and Cisco Unified Communications Manager  B-13
  Codecs, Port Numbers, and IP Addresses  B-14
  Multicast MOH Transmission  B-16
MOH from a Live Feed  B-16
MOH from Flash Files  B-17

How to Use Cisco Unified SRST Gateways as a Multicast MOH Resource  B-18
  Configuring Cisco Unified Communications Manager for Cisco Unified SRST Multicast MOH  B-18
    Configuring the MOH Audio Source to Enable Multicasting  B-19
    Enabling Multicast on the Cisco Unified Communications Manager MOH Server and Configuring Port Numbers and IP Addresses  B-20
    Creating an MRG and an MRGL, Enabling MOH Multicast, and Configuring Gateways  B-23
    Creating a Region for the MOH Server  B-25
  Verifying Cisco Unified Communications Manager Multicast MOH  B-26
  Configuring Cisco Unified SRST for Multicast MOH from an Audio File  B-26
    Prerequisites  B-27
    Enabling Multicast MOH on the Cisco Unified SRST Gateway  B-27
    Verifying Basic Cisco Unified SRST Multicast MOH Streaming  B-31
    Verifying Cisco Unified SRST MOH to PSTN  B-32
    Verifying Cisco Unified SRST Multicast MOH to IP Phones  B-36
  Troubleshooting Tips  B-36
  Configuring Cisco Unified SRST for MOH from a Live Feed  B-36
    Prerequisites  B-37
    Restrictions  B-37
    Setting Up the Voice Port on the Cisco Unified SRST Gateway  B-37
    Setting Up the Directory Numbers on the Cisco Unified SRST Gateway  B-39
    Establishing the MOH Feed  B-39
    Verifying Cisco Unified SRST MOH Live Feed  B-41
  Configurations Examples for Cisco Unified SRST Gateways  B-41
    MOH Routed to Two IP Addresses: Example  B-41
    MOH Live Feed: Example  B-42
  Feature Information for Cisco Unified SRST as a Multicast MOH Resource  B-42
  Where to Go Next  B-43
Preface

This preface describes the audience and conventions of the Cisco Unified SCCP and SIP SRST System Administration Guide. It also describes the available product documentation and provides information on how to obtain documentation and technical assistance.

- Audience, page i
- Conventions, page i
- Obtain Documentation and Submit a Service Request, page ii

Audience

This guide is intended primarily for network administrators and channel partners.

Conventions

This guide uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords.</td>
<td><strong>boldface font</strong></td>
</tr>
<tr>
<td>Variables for which you supply values.</td>
<td><em>italic font</em></td>
</tr>
<tr>
<td>Optional command keywords. You do not have to select any options.</td>
<td>[enclosed in brackets]</td>
</tr>
<tr>
<td>Required command keyword to be selected from a set of options. You must choose one option.</td>
<td>{options enclosed in braces</td>
</tr>
<tr>
<td>Displayed session and system information.</td>
<td><strong>screen font</strong></td>
</tr>
<tr>
<td>Information you enter.</td>
<td><strong>boldface screen font</strong></td>
</tr>
<tr>
<td>Variables you enter.</td>
<td><em>italic screen font</em></td>
</tr>
<tr>
<td>Menu items and button names.</td>
<td><strong>boldface font</strong></td>
</tr>
<tr>
<td>Choosing a menu item.</td>
<td><strong>Option &gt; Network Preferences</strong></td>
</tr>
</tbody>
</table>
Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.
Cisco Unified Survivable Remote Site Telephony Feature Roadmap

This chapter contains a list of Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) features and the location of feature documentation.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Contents

- Documentation Organization, page iv
- Feature Roadmap, page v
- Information About New Features in Cisco Unified SRST, page xi
- Where to Go Next, page xlv
### Documentation Organization

This document consists of the following chapters or appendixes as shown in Table iii-1.

<table>
<thead>
<tr>
<th>Chapter or Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Unified SRST Feature Overview, page 1</strong></td>
<td>Gives a brief description of Cisco Unified SRST and provides information on the supported platforms and Cisco Unified IP Phones. In addition, it describes any prerequisites or restrictions that should be addressed before Cisco Unified SIP SRST is configured.</td>
</tr>
<tr>
<td><strong>Setting Up the Network, page 123</strong></td>
<td>Describes how to set up a Cisco Unified SRST system to communicate with your network.</td>
</tr>
<tr>
<td><strong>Cisco Unified Enhanced Survivable Remote Site Telephony, page 95</strong></td>
<td>Describes how to configure the Cisco Unified Enhanced SRST feature in your network.</td>
</tr>
<tr>
<td><strong>Cisco Unified SIP SRST 4.1, page 135</strong></td>
<td>Describes the features for Cisco Unified SIP SRST Version 4.1 and provides the associated configuration procedures.</td>
</tr>
<tr>
<td><strong>Setting Up Cisco Unified IP Phones using SCCP, page 145</strong></td>
<td>Describes how to set up the basic Cisco Unified SRST phone configuration.</td>
</tr>
<tr>
<td><strong>Setting Up Cisco Unified IP Phones using SIP, page 165</strong></td>
<td>Describes features available in Version 3.0 that are also necessary for Version 3.4. Features include instructions on how to provide a backup to an external SIP call control (IP-PBX) by providing basic registrar services. These services are used by a SIP IP phone in the event of a WAN connection outage when the SIP phone is unable to communicate with its primary SIP proxy.</td>
</tr>
<tr>
<td><strong>Configuring Call Handling, page 183</strong></td>
<td>Describes how to configure incoming and outgoing calls.</td>
</tr>
<tr>
<td><strong>Configuring Secure SRST for SCCP and SIP, page 239</strong></td>
<td>Describes the Secure SRST security functionality to the Cisco Unified SRST.</td>
</tr>
<tr>
<td><strong>Integrating Voicemail with Cisco Unified SRST, page 331</strong></td>
<td>Describes how to set up voicemail.</td>
</tr>
<tr>
<td><strong>Setting Video Parameters, page 355</strong></td>
<td>Describes how to set up video parameters.</td>
</tr>
<tr>
<td><strong>Monitoring and Maintaining Cisco Unified SRST, page 369</strong></td>
<td>Provides a list of useful show commands for monitoring and maintaining Cisco Unified SRST.</td>
</tr>
<tr>
<td><strong>Configuring Cisco Unified SIP SRST Features Using Redirect Mode, page 1</strong></td>
<td>Describes features using redirect mode, which applies to version 3.0 only.</td>
</tr>
<tr>
<td><strong>Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource, page 11</strong></td>
<td>Describes how to configure Cisco Unified CM and Cisco Unified SRST to enable multicast music-on-hold (MOH).</td>
</tr>
</tbody>
</table>
## Feature Roadmap

Table iii-2 provides a feature history summary of Cisco Unified SRST features.

### Table iii-2 Features by Cisco Unified SRST Software Version

<table>
<thead>
<tr>
<th>Cisco Unified SRST</th>
<th>Cisco IOS Release</th>
<th>Enhancements or Modifications</th>
</tr>
</thead>
</table>
|                    |                         | • Toll Fraud Prevention for SIP Line Side on Unified SRST, page 60  
|                    |                         | • Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy, page 57                 |
| Version 12.5       | Cisco IOS XE Gibraltar 16.10.1a | • Support for Unified SRST on Cisco 4461 Integrated Services Routers                              |
| Version 12.3       | Cisco IOS XE Fuji 16.9.1 | • Secure SCCP SRST on Cisco 4000 Series Integrated Services Router, page 243                     |
| Version 12.2       | Cisco IOS XE Fuji 16.8.1 | • Unified E-SRST with Support for Voice Hunt Group, page 96                                       |
| Version 12.1       | Cisco IOS XE Fuji 16.7.1 | • Cisco Smart License, page 13  
|                    |                         | • Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router, page 242              
|                    |                         | • Unified SRST and Unified Border Element Co-location, page 313                                 |
| Version 12.0       | Cisco IOS XE Everest 16.6.1 | • IPv6 Support for Unified SRST SIP IP Phones, page 17                                           |
| Version 11.0       | 15.6(1)T                 | • Support for Cisco IP Phone 7811  
|                    |                         | • Support for Cisco IP Phones 8811, 8831, 8841, 8845, 8865, 8851, 8851NR, 8861                  
|                    |                         | • Support for Cisco ATA-190 Phones                                                              |
| Version 10.5       | 15.4(3)M                 | • Unified E-SRST Scale Support, page 122                                                          |
|                    |                         | • Support for Cisco Unified DX650 SIP IP Phones, page xiii                                      
|                    |                         | • Support for Cisco Unified 78xx SIP IP Phones, page xiii                                      
<p>|                    |                         | • Support for Cisco IP Phones 88xx, 8941, 8945, and 8961                                        |
| Version 10.0       | 15.3(3)M                 | • Cisco Jabber for Windows, page xiii                                                            |
|                    |                         | • SIP: Configure Unified E-SRST, page 99                                                          |
|                    |                         | • To obtain an account on Cisco.com, go to <a href="http://www.cisco.com">www.cisco.com</a> and click Register at the top of the screen., page 4 |</p>
<table>
<thead>
<tr>
<th>Cisco Unified SRST</th>
<th>Cisco IOS Release</th>
<th>Enhancements or Modifications</th>
</tr>
</thead>
</table>
| Version 9.5       | 15.3(2)T         | • After-hour Pattern Blocking Support for Regular Expressions, page xiv  
                      • Call Park Recall Enhancement, page xv  
                      • Display Support for Name of Called Voice Hunt Groups, page xvi  
                      • Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups, page xvii  
                      • Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones, page xviii |
| Version 9.1       | 15.2(4)M         | • KEM Support for Cisco Unified SIP IP Phones, page xxvi  
                      • Enhancement in Speed-Dial Support, page xxvi  
                      • Voice Hunt Group Support, page xxvi |
| Version 9.0       | 15.2(2)T         | • Support for Cisco Unified 6901 and 6911 SIP IP Phones, page xxvii  
                      • Support for Cisco Unified 6921, 6941, 6945, and 6961 SIP IP Phones, page xxviii  
                      • Support for Cisco Unified 8941 and 8945 SIP IP Phones, page xxviii  
                      • Multiple Calls Per Line, page xxviii  
                      • Voice and Fax Support on Cisco ATA-187, page xxix |
| Version 8.8       | 15.2(1)T         | Support for Cisco Unified 6945, 8941, and 8945 SCCP IP Phones, page xxix |
| Version 8.6       | 15.1(4)M         | Support for Cisco Unified 8941 and 8945 SCCP IP Phones were introduced. For more information, see Configuring Cisco Unified 8941 and 8945 SCCP IP Phones, page 148. |
| Version 8.0       | 15.1(1)T         | Beginning with Cisco IP Phone firmware 8.5(3) and Cisco IOS Release 15.1(1)T, Cisco SRST supports SIP signaling over UDP, TCP, and TLS connections, providing both RTP and SRTP media connections based on the security settings of the IP phone. For more information, see the following sections:  
                      • Signaling Security on Unified SRST - TLS, page 246  
                      • Media Security on Unified SRST - SRTP, page 251  
                      • Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293 |
| Version 7.0/4.3   | See Cisco Feature Navigator for compatibility. | • Configuring Eight Calls per Button (Octo-Line), page 158  
                      • Configuring Consultative Transfer, page 195 |
Table iii-2  Features by Cisco Unified SRST Software Version (continued)

<table>
<thead>
<tr>
<th>Cisco Unified SRST</th>
<th>Cisco IOS Release</th>
<th>Enhancements or Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 4.2(1)</td>
<td>See Cisco Feature Navigator for compatibility.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enhanced 911 Services, page 138</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following new features are included:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Assigning ERLs to zones to enable routing to the PSAP that is closest to the caller.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Customizing E911 by defining a default ELIN, identifying a designated number if the 911 caller cannot be reached on callback, specifying the expiry time for data in the Last Caller table, and enabling syslog messages that announce all emergency calls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Expanding the E911 location information to include name and address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Adding new permanent call detail records.</td>
<td></td>
</tr>
<tr>
<td>Version 4.1</td>
<td>12.4(15)T</td>
<td>• Enabling KPML for SIP Phones, page 139</td>
</tr>
<tr>
<td></td>
<td>• Disabling SIP Supplementary Services for Call Forward and Call Transfer, page 138</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configuring Idle Prompt Status for SIP Phones, page 142</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enhanced 911 Services, page 138</td>
<td></td>
</tr>
<tr>
<td>Version 4.0</td>
<td>12.4(4)XC</td>
<td>• Cisco IP Communicator Support, page xxxi</td>
</tr>
<tr>
<td></td>
<td>• Fax Pass-through using SCCP and ATAs Support, page xxxi</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• H.323 VoIP Call Preservation Enhancements for WAN Link Failures for SCCP Phones, page xxxi</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Video Support, page xxxi</td>
<td></td>
</tr>
<tr>
<td>Version 3.4</td>
<td>12.4(4)T</td>
<td>• Cisco SIP SRST 3.4, page xxxii</td>
</tr>
<tr>
<td></td>
<td>• Configuring Cisco Unified SIP SRST Features Using Redirect Mode, page 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configuring Call Handling, page 183 (see Back-to-Back User Agent Mode)</td>
<td></td>
</tr>
<tr>
<td>Version 3.3</td>
<td></td>
<td>• Secure SRST, page xxxii.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified IP Phone 7970G and Cisco Unified 7971G-GE Support, page xxxiii</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enhancement to the show ephone Command, page xxxiii</td>
<td></td>
</tr>
<tr>
<td>Version 3.2</td>
<td>12.3(11)T</td>
<td>• Enhancement to the alias Command, page xxxiii</td>
</tr>
<tr>
<td></td>
<td>• Enhancement to the pickup Command, page xxxiv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enhancement to the user-locale Command, page xxxiv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Increased the Number of Cisco Unified IP Phones Supported on the Cisco 3845, page xxxiv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MOH Live-Feed Support, page xxxiv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No Timeout for Call Preservation, page xxxv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RFC 2833 DTMF Relay Support, page xxxv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Translation Profile Support, page xxxv</td>
<td></td>
</tr>
<tr>
<td>Version 3.1</td>
<td>12.3(7)T</td>
<td>• Cisco Unified IP Phone 7920 Support, page xxxvi</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified IP Phone 7936 Support, page xxxvi</td>
<td></td>
</tr>
</tbody>
</table>
### Table III-2  Features by Cisco Unified SRST Software Version (continued)

<table>
<thead>
<tr>
<th>Cisco Unified SRST</th>
<th>Cisco IOS Release</th>
<th>Enhancements or Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 3.0</td>
<td>12.2(15)ZJ</td>
<td>• Additional Language Options for IP Phone Display, page xxxvi</td>
</tr>
<tr>
<td></td>
<td>12.3(4)T</td>
<td>• Consultative Call Transfer and Forward Using H.450.2 and H.450.3 for SCCP Phones, page xxxvii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customized System Message for Cisco Unified IP Phones, page xxxvii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dual-Line Mode, page xxxvii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• E1 R2 Signaling Support, page xxxviii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• European Date Formats, page xxxix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Huntstop for Dual-Line Mode, page xxxix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Music-on-Hold for Multicast from Flash Files, page xxxix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ringing Timeout Default, page xxxix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Secondary Dial Tone, page xxxix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enhancement to the show ephone Command, page xl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System Log Messages for Phone Registrations, page xl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Three-Party G.711 Ad Hoc Conferencing, page xl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for Cisco VG248 Analog Phone Gateway 1.2(1) and Higher Versions, page xl</td>
</tr>
<tr>
<td>Version 2.1</td>
<td></td>
<td>• Cisco Unified IP Phone 7902G Support, page xlii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified IP Phone 7912G Support, page xlii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Additional Language Options for IP Phone Display, page xlii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco SRST Aggregation, page xlii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco ATA 186 and ATA 188 Support, page xlii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified IP Phone 7905G Support, page xlii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified IP Phone Expansion Module 7914 Support, page xliii</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enhancement to the dialplan-pattern Command, page xliii</td>
</tr>
<tr>
<td>Version 2.02</td>
<td></td>
<td>• Cisco Unified IP Phone Conference Station 7935 Support, page xlv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Increase in Directory Numbers, page xlv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unity Voice Mail Integration Using In-Band DTMF Signaling Across the PSTN and BRI PRI, page xlv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified SRST was implemented on the Cisco Catalyst 4500 access gateway module and Cisco 7200 routers (NPE-225, NPE-300, and NPE-400).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support was removed for the Cisco MC3810 V3 concentrator.</td>
</tr>
<tr>
<td>Version 2.01</td>
<td></td>
<td>• Cisco Unified SRST was implemented on the Cisco 1760 routers, and support for the Cisco 1750 was removed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support was added for additional connected Cisco IP phones.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support was added for additional directory numbers or virtual voice ports on Cisco IP phones.</td>
</tr>
</tbody>
</table>
### Table iii-2  Features by Cisco Unified SRST Software Version (continued)

<table>
<thead>
<tr>
<th>Cisco Unified SRST</th>
<th>Cisco IOS Release</th>
<th>Enhancements or Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 2.0</td>
<td></td>
<td>• Cisco Unified SRST was implemented on the Cisco 2600XM and Cisco 2691 routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified SRST was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725 and Cisco 3745 routers and the Cisco MC3810-V3 concentrators.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified SRST was implemented on the Cisco 1750 and Cisco 1751 routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Huntstop support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Class of restriction (COR).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Translation rule support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MOH and tone on hold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distinctive ringing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Forward to a central voicemail or auto-attendant (AA) through PSTN during Cisco Unified Communications Manager fallback.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Phone number alias support during Cisco Unified Communications Manager fallback: enhanced default destination support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• List-based call restrictions for Cisco Unified Communications Manager fallback.</td>
</tr>
</tbody>
</table>
## Feature Roadmap

**Version 1.0**
- Support was added for 144 Cisco IP phones on the Cisco 3660 multiservice routers.
- Cisco Unified SRST introduced on the Cisco 2600 series and Cisco 3600 series multiservice routers and the Cisco IAD2420 series integrated access devices.
- Cisco IP phones able to establish a connection with an SRST router in the event of a WAN link to Cisco Unified Communications Manager failure.
- Dimming of all Cisco Unified IP Phone function keys that are not supported during Cisco Unified SRST operation.
- Extension-to-extension dialing.
- Direct Inward Dialing (DID).
- Direct Outward Dialing (DOD).
- Calling party ID (Caller ID/ANI) display.
- Last number redial.
- Preservation of local extension-to-extension calls when WAN link fails.
- Preservation of local extension to PSTN calls when WAN link fails.
- Preservation of calls in progress when failed WAN link is re-established.
- Blind transfer of calls within IP network.
- Multiple lines per Cisco IP phone.
- Multiple-line appearance across telephones.
- Call hold (shared lines).
- Analog Foreign Exchange Station (FXS) and Foreign Exchange Office (FXO) ports.
- BRI support for EuroISDN.
- PRI support for NET5 switch type.

### Table iii-2 Features by Cisco Unified SRST Software Version (continued)

<table>
<thead>
<tr>
<th>Cisco Unified SRST</th>
<th>Cisco IOS Release</th>
<th>Enhancements or Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td></td>
<td>• Support was added for 144 Cisco IP phones on the Cisco 3660 multiservice routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Unified SRST introduced on the Cisco 2600 series and Cisco 3600 series multiservice routers and the Cisco IAD2420 series integrated access devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco IP phones able to establish a connection with an SRST router in the event of a WAN link to Cisco Unified Communications Manager failure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dimming of all Cisco Unified IP Phone function keys that are not supported during Cisco Unified SRST operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Extension-to-extension dialing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Direct Inward Dialing (DID).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Direct Outward Dialing (DOD).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Calling party ID (Caller ID/ANI) display.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Last number redial.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Preservation of local extension-to-extension calls when WAN link fails.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Preservation of local extension to PSTN calls when WAN link fails.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Preservation of calls in progress when failed WAN link is re-established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Blind transfer of calls within IP network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple lines per Cisco IP phone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple-line appearance across telephones.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Call hold (shared lines).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Analog Foreign Exchange Station (FXS) and Foreign Exchange Office (FXO) ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• BRI support for EuroISDN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PRI support for NET5 switch type.</td>
</tr>
</tbody>
</table>
Information About New Features in Cisco Unified SRST

This section contains the following topics:

- New Features for Unified SRST Version 12.6, page xi
- New Features for Unified SRST Version 12.3, page xi
- New Features for Unified SRST Version 12.2, page xii
- New Features for Unified SRST Version 12.1, page xii
- New Feature for Unified SRST Version 12.0, page xii
- New Features for Cisco Unified SRST Version 11.0, page xii
- New Features in Cisco Unified SRST Version 10.5, page xii
- New Features in Cisco Unified SRST Version 10.0, page xiii
- New Features in Cisco Unified SRST Version 9.5, page xiv
- New Features in Cisco Unified SRST Version 9.1, page xxv
- New Features in Cisco Unified SRST Version 9.0, page xxvii
- New Features in Cisco Unified SRST Version 8.8, page xxix
- New Features in Cisco Unified SRST Version 8.0, page xxix
- New Features in Cisco Unified SRST Version 7.0/4.3, page xxix
- New Features in Cisco SRST Version 4.2(1), page xxx
- New Features in Cisco Unified SRST Version 4.1, page xxx
- New Features in Cisco Unified SRST Version 4.0, page xxx
- New Features in Cisco Unified SRST Version 3.4, page xxxii
- New Features in Cisco SRST Version 3.3, page xxxii
- New Features in Cisco SRST Version 3.2, page xxxiii
- New Features in Cisco SRST Version 3.1, page xxxv
- New Features in Cisco SRST Version 3.0, page xxxvi
- New Features in Cisco SRST Version 2.1, page xl
- New Features in Cisco SRST Version 2.02, page xlv

New Features for Unified SRST Version 12.6

Unified SRST 12.6 Release introduces support for the following new features:

- Simple Network Management Protocol (SNMP) Support for Unified SRST, page 40
- Toll Fraud Prevention for SIP Line Side on Unified SRST, page 60
- Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy, page 57

New Features for Unified SRST Version 12.3

Unified SRST 12.3 Release introduces support for the following new feature:
New Features for Unified SRST Version 12.2

Unified SRST 12.2 Release introduces support for the following new feature:

- Unified E-SRST with Support for Voice Hunt Group, page 96

New Features for Unified SRST Version 12.1

Unified SRST 12.1 introduces support for the following new features:

- Cisco Smart License, page 13
- Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router, page 242
- Unified SRST and Unified Border Element Co-location, page 313

New Feature for Unified SRST Version 12.0


New Features for Cisco Unified SRST Version 11.0

Cisco Unified SRST 11.0 supports the following new Cisco IP phones and adapters:

- Support for Cisco IP Phone 7811
- Support for Cisco IP Phones 8811, 8831, 841, 8851, 8851NR, 8861
- Support for Cisco ATA-190

For information on the phones supported in Cisco Unified SRST 11.0, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

New Features for Cisco Unified SRST Version 10.5

Cisco Unified SRST 10.5 supports the following features:

- Unified E-SRST Scale Support, page 122

For more information on the Cisco Unified SRST 10.5 supported feature, see the “SCCP: Configure Unified E-SRST” section on page 115.

Cisco Unified SRST 10.5 supports the following new Cisco Unified SIP IP phones:

- Support for Cisco Unified DX650 SIP IP Phones, page xiii
- Support for Cisco Unified 78xx SIP IP Phones, page xiii

- Secure SCCP SRST on Cisco 4000 Series Integrated Services Router, page 243
Support for Cisco Unified DX650 SIP IP Phones

For information on feature support for the Cisco Unified DX650 SIP IP Phones in Cisco Unified SRST 10.5, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Support for Cisco Unified 78xx SIP IP Phones

For information on feature support for the Cisco Unified 78xx SIP IP Phones in Cisco Unified SRST 10.5, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

New Features in Cisco Unified SRST Version 10.0

Cisco Unified SRST 10.0 supports the following new features:

- Cisco Jabber for Windows, page xiii
- SIP: Configure Unified E-SRST, page 99

To obtain an account on Cisco.com, go to www.cisco.com and click Register at the top of the screen.

Cisco Jabber for Windows

Cisco Jabber for Windows client is supported from Cisco Unified CME Release 10 onwards. Cisco Jabber for Windows supports the visual voicemail functionality integrated with the Cisco Unity connection. Cisco Jabber for Windows is a SIP-based soft client with integrated Instant Messaging and presence functionality, and uses the new Client Services Framework 2nd Generation (CSF2G) architecture.

CSF is a unified communications engine that is reused by multiple Cisco PC-based clients. The Cisco Jabber client has to be registered with a presence server such as cloud-based Cisco Webex server, or Cisco Unified Presence server to avail the standard XMPP-based instant messaging functionalities. The client is identified by a device ID name that can be configured under the voice register pool in Cisco Unified CME. You should configure the username and password under voice register pool to identify the user logging into Cisco Unified CME through Cisco Jabber for Windows client. The device discovery process uses HTTPS connection. Therefore, you should configure the secure HTTP on Cisco Unified CME. A new phone type, Jabber-Win has been added to configure the voice register pool for Cisco Jabber for Windows client.

Restrictions

- The Cisco Jabber for Windows client version should be version 9.1.0 and later version.
- The Cisco Jabber for Windows client should register with a presence server such as cloud-based Webex server, or a Cisco Unified Presence server to enable the telephony features on the Jabber client.
- The Cisco Jabber for Windows client supports only the visual voicemail functionality using Internet Message Access Protocol (IMAP) on the Cisco Unity Connection.
New Features in Cisco Unified SRST Version 9.5

Cisco Unified SRST 9.5 supports the following new features:

- After-hour Pattern Blocking Support for Regular Expressions, page xiv
- Call Park Recall Enhancement, page xv
- Display Support for Name of Called Voice Hunt Groups, page xvi
- Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups, page xvii
- Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones, page xviii

After-hour Pattern Blocking Support for Regular Expressions

In Cisco Unified SRST 9.5, support for afterhours pattern blocking is extended to regular expression patterns for dial plans on Cisco Unified SIP and Cisco Unified SCCP IP phones. With this support, users can add a combination of fixed dial plans and regular expression-based dial plans.

When a call is initiated after hours, the dialed number is matched against a combination of dial plans. If a match is found, the call is blocked.

To enable regular expression patterns to be included when configuring afterhours pattern blocking, the `after-hours block pattern` command is modified to include regular expressions as a value for the `pattern` argument in the following command syntax:

```
after-hours block pattern pattern-tag pattern
```

This command is available in the following configuration modes:

- telephony-service—For both SCCP and SIP Phones.
- ephone-template—For SCCP phones only.

Note

The maximum length of a regular expression pattern is 32 for both Cisco Unified SIP and Cisco Unified SCCP IP phones.

If calls to the following numbers are to be blocked after hours:

- numbers beginning with ‘0’ and ‘00’
numbers beginning with 1800, followed by four digits
numbers 9876512340 to 9876512345
then the following configurations can be used:
- after-hours block pattern 1 0*
- after-hours block pattern 2 00*
- after-hours block pattern 3 1800….
- after-hours block pattern 4 987651234[0-5]

Note
There is no change in the number of afterhours patterns that can be added. The maximum number is still 100.

For more information on configuration examples, see the “Configuring Afterhours Block Patterns of Regular Expressions: Example” section of Cisco Unified Communications Manager Administration Guide.

For a summary of the basic Cisco IOS regular expression characters and their functions, see the “Cisco Regular Expression Pattern Matching Characters” section of Terminal Services Configuration Guide.

Call Park Recall Enhancement

Before Cisco Unified CME 9.5, a parked call could not be recalled by or transferred to the phone that put the call in park or the original phone that transferred the call when the destination phone was offhook or ringing.

In Cisco Unified CME 9.5, the recall force keyword is added to the call-park system command in telephony-service configuration mode to allow a user to force the recall or transfer of a parked call to the phone that put the call in park or the phone with the reserved-for number as its primary DN when the destination phone is available to answer the call.

In Cisco Unified CME 10.5, a new ring tone is introduced for park recall to assist the phone user to distinctly identify the type of call.

This feature is supported on all phone families for SCCP endpoints and on 89XX and 99XX phone families for SIP endpoints. No configurations are required to activate this feature.

Examples

The following example configures the Call Park Recall:

Router# configure terminal
Router(config)# telephony-service
Router(config)# srst mode auto-provision all
Router(config-telephony)# call-park system ? recall Configure parameters for recall
Router(config-telephony)# call-park system recall ? force Force recall for busy call park initiator
Router(config-telephony)# call-park system recall force
**Park Monitor**

In Cisco Unified CME 8.5 and later versions, the park monitor feature allows you to park a call and monitor the status of the parked call until the parked call is retrieved or abandoned. When a Cisco Unified SIP IP Phone 8961, 9951, or 9971 parks a call using the park soft key, the park monitoring feature monitors the status of the parked call. The park monitoring call bubble is not cleared until the parked call gets retrieved or is abandoned by the parkee. This parked call can be retrieved using the same call bubble on the parker’s phone to monitor the status of the parked call.

Once a call is parked, Cisco Unified CME sends a SIP NOTIFY message to the parker phone indicating the “parked” event along with the park slot number so that the parker phone can display the park slot number as long as the call remains parked.

When a parked call is retrieved, Cisco Unified CME sends another SIP NOTIFY message to the parker phone indicating the “retrieved” event so that the phone can clear the call bubble. When a parked call is disconnected by the parkee, Cisco Unified CME sends a SIP NOTIFY message to the parker phone indicating the “abandoned” event and the parker phone clears the call bubble upon cancellation of the parked call.

When a parked call is recalled or transferred, Cisco Unified CME sends a SIP NOTIFY message to the parker phone indicating the “forwarded” event so that parker phone can clear the call bubble during park, recall, and transfer. You can also retrieve a parked call from the parker phone by directly selecting the call bubble or pressing the resume soft key on the phone.

**Display Support for Name of Called Voice Hunt Groups**

A voice hunt group is associated with a pilot number. But because there is no association with the name of the voice hunt group when calls are forwarded from the voice hunt group to the final number, the forwarding number is sent without the name of the forwarding party. The final number can be in the form of a voicemail, a Basic Automatic Call Distribution (BACD) script, or another extension.

In Cisco Unified SRST 9.5, the display of the name of the called voice-hunt-group pilot is supported by configuring the following command in voice hunt-group or ephone-hunt configuration mode:

```
[no] name "primary pilot name" [secondary "secondary pilot name"]
```

The secondary name is optional and when the secondary pilot name is not explicitly configured, the primary pilot name is applicable to both pilot numbers.

For configuration information, see the “Associating a Name with a Called Voice Hunt Group” section.

**Examples**

The following example configures the primary pilot name for both the primary and secondary pilot numbers:

```
name SALES
```

The following example configures different names for the primary and secondary pilot numbers:

```
name SALES secondary SALES-SECONDARY
```

**Note**

Use quotes (") when input strings have spaces in between as shown in the next three examples.
The following example associates a two-word name for the primary pilot number and a one-word name for the secondary pilot number:

```
name "CUSTOMER SERVICE" secondary CS
```

The following example associates a one-word name for the primary pilot number and a two-word name for the secondary pilot number:

```
name FINANCE secondary "INTERNAL ACCOUNTING"
```

The following example associates two-word names for the primary and secondary pilot numbers:

```
name "INTERNAL LLER" secondary "EXTERNAL LLER"
```

For configuration information, see the “Associating a Name with a Called Voice Hunt Group” section of *Cisco Unified Communications Manager Administration Guide*.

For configuration examples, see the “Example: Associating a Name with a Called Voice Hunt Group” section of *Cisco Unified Communications Manager Administration Guide*.

**Restrictions**

- Display support applies to Cisco Unified SCCP IP phones in voice hunt-group and ephone-hunt configuration modes but are not supported in Cisco Unified SIP IP phones.
- Called name and called number information displayed on the caller’s phone follows existing behavior, where the called names and called numbers are updated so that a sequential hunt reflects the name and number of the ringing phone.

### Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups

Local or internal calls are calls originating from a Cisco Unified SIP or Cisco Unified SCCP IP phone in the same Cisco Unified CME system.

Before Cisco Unified CME 9.5, the `no forward local-calls` command was configured in ephone-hunt group to prevent a local call from being forwarded to the next agent.

In Cisco Unified CME 9.5, local calls are prevented from being forwarded to the final destination using the `no forward local-calls to-final` command in parallel or sequential voice hunt-group configuration mode.

When the `no forward local-calls to-final` command is configured in sequential voice hunt-group configuration mode, local calls to the hunt-group pilot number are sent sequentially only to the list of members of the group using the rotary-hunt technique. In case all the group members of the voice hunt group are busy, the caller hears a busy tone. If any of the group members are available but do not answer, the caller hears a ringback tone and is eventually disconnected after the specified timeout. The call is not forwarded to the final number.

When the `no forward local-calls to-final` command is configured in parallel voice hunt-group configuration mode, local calls to the hunt-group pilot number are sent simultaneously to the list of members of the group using the blast technique. In case all the group members of the voice hunt group are busy, the caller hears a busy tone. If any of the group members are available but do not answer, the caller hears a ringback tone and is eventually disconnected after the specified timeout. The call is not forwarded to the final number. For configuration examples, see the “Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups” section of *Cisco Unified Communications Manager Administration Guide*.
Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones

In Cisco Unified Survivable Remote Site Telephony (SRST) 4.0, trunk-to-trunk transfer blocking for toll bypass fraud prevention is supported on Cisco Unified Skinny Client Control Protocol (SCCP) IP phones.

Table iii-3 lists the transfer-blocking commands and the appropriate configuration modes for Cisco Unified CME and Cisco Unified SRST.

### Table iii-3 Configuration Modes for Transfer-Blocking Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Cisco Unified SRST</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer-pattern</td>
<td>call-manager-fallback</td>
</tr>
<tr>
<td>transfer max-length</td>
<td>voice register pool</td>
</tr>
<tr>
<td>transfer-pattern blocked</td>
<td>voice register pool</td>
</tr>
<tr>
<td>conference transfer-pattern</td>
<td>call-manager-fallback</td>
</tr>
<tr>
<td>conference max-length</td>
<td>voice register pool or voice register template</td>
</tr>
<tr>
<td>conference-pattern blocked</td>
<td>voice register pool or voice register template</td>
</tr>
</tbody>
</table>

**Note**
The call transfer and conference restrictions apply when transfers or conferences are initiated toward external parties, like a PSTN trunk, a SIP trunk, or an H.323 trunk. The restrictions do not apply to transfers and conferences to local extensions.

#### transfer-pattern

The `transfer-pattern` command for Cisco Unified SIP IP phones functions like the `transfer-pattern` command for Cisco Unified SCCP IP phones by allowing all, not just local, transfers to take place. The `transfer-pattern` command specifies the directory numbers for call transfer. The command can be configured up to 32 times using the following command syntax: `transfer-pattern transfer-pattern [blind].`

**Note**
The `blind` keyword in the `transfer-pattern` command applies only to Cisco Unified SCCP IP phones and does not apply to Cisco Unified SIP IP phones.

With the `transfer-pattern` command configured, only call transfers to numbers that match the configured transfer pattern are allowed to take place. With the transfer pattern configured, all or a subset of transfer numbers can be dialed and the transfer to a remote party can be initiated.

The following are examples of configurable transfer patterns:

- .T—This configuration allows call transfers to any destinations with one or more digits, like 123, 877656, or 76548765.
• 919...—This configuration only allows call transfers to remote numbers beginning with “919” and followed by eight digits, like 91912345678. However, call transfers to 9191234 or 919123456789 are not allowed.

**Backward Compatibility**

To maintain backward compatibility, all call transfers from Cisco Unified SIP IP phones to any number (local or over trunk) are allowed when no transfer patterns are configured through the `transfer-pattern`, `transfer-pattern blocked`, or `transfer max-length` commands.

For Cisco Unified SCCP IP phones, call transfers over trunk continue to be blocked when no transfer patterns are configured.

**Dial Plans**

Whatever dial plan is used for external calls, the same numbers should be configured as specific numbers using the `transfer-pattern` command.

If a dial plan requires “9” to be dialed before an external call is made, then “9” should be a prefix of the transfer-pattern number. For example, if 12345678 is an external number that requires “9” to be dialed before the external call can be made, then the transfer-pattern number should be 912345678.

**transfer max-length**

The `transfer max-length` command is used to indicate the maximum length of the number being dialed for a call transfer. When only a specific number of digits are to be allowed during a call transfer, a value between 3 and 16 is configured. When the number dialed exceeds the maximum length configured, then the call transfer is blocked.

For example, if the maximum length is configured as 5, then only call transfers from Cisco Unified SIP IP phones up to a five-digit directory number are allowed. All call transfers to directory numbers with more than five digits are blocked.

---

**Note**

If only transfer max length is configured and conference max-length is not configured, then transfer max-length takes effect for transfers and conferences.

**transfer-pattern blocked**

When the `transfer-pattern blocked` command is configured for a specific phone, no call transfers are allowed from that phone over the trunk.

This feature forces unconditional blocking of all call transfers from the specific phone to any other non-local numbers (external calls from one trunk to another trunk). No call transfers from this specific phone are possible even when a transfer pattern matches the dialed digits for transfer.

Table iii-4 compares the behaviors of Cisco Unified SCCP and SIP IP phones for specific configurations.
conference-pattern blocked

The `conference-pattern blocked` command is used to prevent extensions on a voice register pool from initiating conferences.

The following table summarizes the behavior of the `conference-pattern blocked` command in relation to `no conference-pattern blocked`, `conference max-length`, `no conference max-length`, and `transfer max-length` commands.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Cisco Unified SCCP IP Phones</th>
<th>Cisco Unified SIP IP Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>No transfer patterns are configured.</td>
<td>All non-local call transfers are blocked.</td>
<td>All non-local call transfers are allowed for backward compatibility.</td>
</tr>
<tr>
<td>Specific transfer patterns are configured.</td>
<td>Call transfers to specific external entities are allowed.</td>
<td>Call transfers to specific external entities are allowed.</td>
</tr>
<tr>
<td>The <code>transfer-pattern blocked</code> command is configured.</td>
<td>All non-local call transfers are blocked.</td>
<td>All non-local call transfers are blocked.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The configuration reverts to the default, where no transfer patterns are configured.</td>
<td>The configuration unconditionally blocks all non-local call transfers. It does not return to the default, where all non-local call transfers are allowed.</td>
</tr>
</tbody>
</table>

### conference-pattern blocked

The `conference-pattern blocked` command is used to prevent extensions on a voice register pool from initiating conferences.

The following table summarizes the behavior of the `conference-pattern blocked` command in relation to `no conference-pattern blocked`, `conference max-length`, `no conference max-length`, and `transfer max-length` commands.

<table>
<thead>
<tr>
<th>configuration</th>
<th>conference max-length</th>
<th>no conference max-length</th>
</tr>
</thead>
<tbody>
<tr>
<td>No conference-pattern blocked (default case)</td>
<td>Allowing/Blocking of conference call depends on configured conference max-length</td>
<td>Allowing/Blocking of conference call depends on configured transfer max-length</td>
</tr>
<tr>
<td>conference-pattern blocked</td>
<td>Conference calls are not allowed on SIP and SCCP phones.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Max-length &lt;= allowed max-length</th>
<th>Max-length &gt; allowed max-length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer</td>
<td>Conference</td>
</tr>
<tr>
<td><strong>Y</strong></td>
<td><strong>Y</strong></td>
</tr>
</tbody>
</table>

Transfer max-length +
No Conference max-length (use transfer max-length for conference cases too, as conference max-length not configured)
### Configuring the Maximum Number of Digits for a Conference Call

This feature enables you to specify the maximum number of digits while making a conference call.

#### Prerequisites

- Cisco Unified SRST 10.5 or a later version.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice register pool pool-tag`
4. `conference max-length value`
5. `end`

<table>
<thead>
<tr>
<th>No transfer max-length + Conference max-length (conference max-length has precedence over transfer max-length for conference)</th>
<th>Max-length &lt;= allowed max-length</th>
<th>Max-length &gt; allowed max-length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>No transfer max-length + Conference max-length (conference max-length has precedence over transfer max-length for conference)</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>No transfer max-length + No conference max-length</td>
<td>All transfer and conference calls are allowed</td>
<td>N</td>
</tr>
</tbody>
</table>
**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>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register pool pool-tag or ephone phone-tag</td>
<td>Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME or for a set of Cisco Unified SIP IP phones in Cisco Unified SIP SRST.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice register pool 25</td>
<td></td>
</tr>
<tr>
<td>pool-tag</td>
<td>Unique number assigned to the pool. Range is 1 to 100.</td>
</tr>
<tr>
<td><strong>or</strong></td>
<td></td>
</tr>
<tr>
<td>template-tag</td>
<td>Declares a template tag. Range is 1 to 10.</td>
</tr>
<tr>
<td><strong>or</strong></td>
<td></td>
</tr>
<tr>
<td>phone-tag</td>
<td>Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type ? to display range.</td>
</tr>
<tr>
<td><strong>Step 4</strong> configure max-length value</td>
<td>Allows the conference of calls from Cisco IP phones to specified directory numbers of phones other than Cisco IP phones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# conference max-length 6</td>
<td></td>
</tr>
<tr>
<td>conference max-length</td>
<td>Allows conference call depending on the configured conference max-length. Range is 3 to 16.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits telephony-service configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Conference Blocking Options for Phones**

This feature prevents extensions from making conference calls to directory numbers that are otherwise allowed globally.
Prerequisites

- Cisco Unified SRST 10.5 or a later version.
- The transfer-pattern command must be configured.
- The conference transfer-pattern command must be configured.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool pool-tag
4. conference-pattern blocked
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> Router&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> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register pool pool-tag</td>
<td>Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME or for a set of Cisco Unified SIP IP phones in Cisco Unified SIP SRST.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config)# voice register pool 25</td>
<td>- <em>pool-tag</em>—Unique number assigned to the pool. Range is 1 to 100.</td>
</tr>
<tr>
<td>or Enters voice register template configuration mode and defines a template of common parameters for Cisco Unified SIP IP phones.</td>
<td></td>
</tr>
<tr>
<td>or Enters ephone configuration mode.</td>
<td></td>
</tr>
<tr>
<td><em>Example:</em> Router(config-telephony)# conference-pattern blocked</td>
<td>- <em>template-tag</em>—Declares a template tag. Range is 1 to 10.</td>
</tr>
<tr>
<td>or Enters ephone configuration mode.</td>
<td></td>
</tr>
<tr>
<td><em>phone-tag</em>—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type ? to display range.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> conference-pattern blocked</td>
<td>Allows the conference of calls from Cisco IP phones to specified directory numbers of phones other than Cisco IP phones.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config-telephony)# conference-pattern blocked</td>
<td>- <em>conference-pattern blocked</em>—No conference calls are allowed.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits telephony-service configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config-telephony)# exit</td>
<td></td>
</tr>
</tbody>
</table>

transfer-pattern blocked

When the **transfer-pattern blocked** command is configured for a specific phone, no call transfers are allowed from that phone over the trunk.

This feature forces unconditional blocking of all call transfers from the specific phone to any other non-local numbers (external calls from one trunk to another trunk). No call transfers from this specific phone are possible even when a transfer pattern matches the dialed digits for transfer.
Table iii-5 compares the behaviors of Cisco Unified SCCP and SIP IP phones for specific configurations.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Cisco Unified SCCP IP Phones</th>
<th>Cisco Unified SIP IP Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>No transfer patterns are configured.</td>
<td>All non-local call transfers are blocked.</td>
<td>All non-local call transfers are allowed for backward compatibility.</td>
</tr>
<tr>
<td>Specific transfer patterns are configured.</td>
<td>Call transfers to specific external entities are allowed.</td>
<td>Call transfers to specific external entities are allowed.</td>
</tr>
<tr>
<td>The transfer-pattern blocked command is configured.</td>
<td>All non-local call transfers are blocked.</td>
<td>All non-local call transfers are blocked.</td>
</tr>
<tr>
<td></td>
<td>Note The configuration reverts to the default, where no transfer patterns are configured.</td>
<td>Note The configuration unconditionally blocks all non-local call transfers. It does not return to the default, where all non-local call transfers are allowed.</td>
</tr>
</tbody>
</table>

conference transfer-pattern

When both the transfer-pattern and conference transfer-pattern commands are configured and dialed digits match the configured transfer pattern, conference calls are allowed. However, when the dialed digits do not match any of the configured transfer pattern, the conference call is blocked.

For information on provisioning Cisco Unified IP phones for secure access to web content using HTTPS, see the “HTTPS Provisioning for Cisco Unified IP Phones” section of Cisco Unified Communications Manager Express System Administrator Guide.

For configuration examples, see the “Configuring HTTPS Support for Cisco Unified CME:Example” section of Cisco Unified Communications Manager Administration Guide.

New Features in Cisco Unified SRST Version 9.1

Cisco Unified SRST 9.1 supports the following new features:

- KEM Support for Cisco Unified SIP IP Phones, page xxvi
- Enhancement in Speed-Dial Support, page xxvi
- Voice Hunt Group Support, page xxvi

Note If you have older routers, such as the VG26nn and VG37nn platforms and Cisco Integrated Services Router (ISR) Generation 1 platforms (Cisco ISR 1861, 2800, and 3800 Series), you need to upgrade to Cisco ISR 881, 886VA, 887VA, 888, 888E, 1861E, 2900, 3900, and 3900E Series platforms to utilize these new features.
KEM Support for Cisco Unified SIP IP Phones

Cisco Unified IP Key Expansion Modules (KEMs) are supported on Cisco Unified 8851/51NR, 8861, 8961, 9951, and 9971 SIP IP phones from Cisco Unified SIP SRST 9.1.

For information on KEM support for Cisco Unified 8851/51NR, 8861, 8961, 9951, and 971 SIP IP phones, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Restrictions

- Bulk registration is not supported for KEMs in Cisco Unified SRST. Phones do not send bulk registration requests but always use the User Datagram Protocol (UDP) port for registration.
- KEM is not supported for Cisco Unified SCCP IP Phones and Cisco Unified SIP IP Phones other than the Cisco Unified 8851/51NR, 8861, 8961, 9951, and 9971 SIP phones.
- Features configured on keys are disabled when supported Cisco Unified SIP IP phones are in Cisco Unified SIP SRST.
- All Cisco Unified 8851/51NR, 8861, 8961, 9951, and 9971 SIP IP phone restrictions and limitations apply to KEMs.
- All Cisco Unified SIP SRST feature restrictions and limitations apply to KEMs.

For more information on how the `blf-speed-dial`, `number`, and `speed-dial` commands, in voice register pool configuration mode, have been modified, see Cisco Unified Communications Manager Express Command Reference.

For information on installing KEMs on Cisco Unified IP Phone, see the “Installing a Key Expansion Module on the Cisco Unified IP Phone” section of Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 7.1 (3) (SIP).

For information on installing KEMs on Cisco Unified 8811, 8841, 8851, 8851NR, and 8861 Phones, see the Cisco IP Phone Key Expansion Module section of Cisco IP Phone 8811, 8841, 8851, 8851NR, and 8861 Administration Guide for Cisco Unified Communications Manager.

Enhancement in Speed-Dial Support

In Cisco Unified SRST 9.1, the “,” or comma (pause indicator) is ignored to avoid a break in speed-dial support.

Because the pause speed-dial feature (supported in Cisco Unified Communications Manager or Cisco Unified CM) is not supported in Cisco Unified SRST, Cisco Unified CM and phones (Cisco Unified SCCP IP phones and Cisco Unified SIP IP phones) registered in Cisco Unified SRST maintain backward compatibility in Cisco Unified SRST mode. When phones failover to the Cisco Unified SRST router during WAN outages and Cisco Unified CM failure, the phones only send the speed-dial numbers when the pause speed-dial buttons are pressed. The comma pause indicator is ignored and the preconfigured FAC, PIN, and DTMF are not sent.

For information on configuring speed-dial in Cisco Unified Communications Manager, see the “Device setup” chapter of Cisco Unified Communications Manager Administration Guide.

Voice Hunt Group Support

Cisco Unified SIP SRST 9.1 supports voice hunt groups. Voice hunt groups allow a call placed to a single (pilot) number to contact multiple destinations.
There are three different types of voice hunt groups. Each type uses a different strategy to determine the first number that rings for successive calls to the pilot number until a number answers.

- **Parallel Hunt Groups**—Allows an incoming call to simultaneously ring all the numbers in the hunt group member list.
- **Sequential Hunt Groups**—Allows an incoming call to ring all the numbers in the left-to-right order in which they were listed when the hunt group was defined. The first number in the list is always the first number tried when the pilot number is called. Maximum number of hops is not a configurable parameter for sequential hunt groups.
- **Longest-Idle Hunt Groups**—Allows an incoming call to first go to the number that has been idle the longest for the number of hops specified when the hunt group was defined. The longest-idle time is determined from the last time that a phone registered, re-registered, or went on-hook.

While ephone hunt groups only support Cisco Unified SCCP IP phones, a voice hunt group supports Cisco Unified SCCP IP phones, Cisco Unified SIP IP phones, or a mixture of Cisco Unified SCCP IP phones and Cisco Unified SIP IP phones.

With the voice hunt group feature preconfigured in the Cisco Unified SIP SRST router, voice hunt groups continue to be supported after phones fallback from Cisco Unified CM to the Cisco Unified SIP SRST router.

**Restrictions**
- Hunt group statistics is not supported for voice hunt groups in Cisco Unified SRST.
- Hunt group nesting or setting the final number of one hunt group as the pilot of another hunt group is not supported.

### New Features in Cisco Unified SRST Version 9.0

Cisco Unified SRST 9.0 supports the following new Cisco Unified SIP IP phones:

- Cisco Unified 6901 and 6911 SIP IP Phones
- Cisco Unified 6921, 6941, 6945, and 6961 SIP IP Phones
- Cisco Unified 8941 and 8945 SIP IP Phones

Cisco Unified SRST 9.0 supports the following new features:

- **Multiple Calls Per Line**, page xxviii
- **Voice and Fax Support on Cisco ATA-187**, page xxix

### Support for Cisco Unified 6901 and 6911 SIP IP Phones

For information on feature support for the Cisco Unified 6901 and 6911 SIP IP Phones in Cisco Unified SRST, see **Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST**.
Support for Cisco Unified 6921, 6941, 6945, and 6961 SIP IP Phones

For information on feature support for the Cisco Unified 6921, 6941, 6945, and 6961 SIP IP Phones in Cisco Unified SRST, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Support for Cisco Unified 8941 and 8945 SIP IP Phones

For information on feature support for the Cisco Unified 8941 and 8945 SIP IP Phones in Cisco Unified SRST, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Multiple Calls Per Line

Cisco Unified SRST 9.0 provides support for the Multiple Calls Per Line (MCPL) feature on Cisco Unified 6921, 6941, 6945, and 6961 SIP IP phones and Cisco Unified 8941 and 8945 SCCP and SIP IP phones.

Before Cisco Unified SRST 9.0, the maximum number of calls supported for every directory number (DN) on Cisco Unified 8941 and 8945 SCCP IP phones was restricted to two.

With Cisco Unified SRST 9.0, the MCPL feature overcomes the limitation on the maximum number of calls per line.

In Cisco Unified SRST 9.0, the MCPL feature is not supported on Cisco Unified 6921, 6941, 6945, and 6961 SCCP IP phones. The maximum number of calls allowed on these phones is two and the maximum number of calls allowed on octo-line directory numbers on these phones before activating Call Forward Busy or a busy tone is one.

Cisco Unified 8941 and 8945 SCCP IP Phones

Before Cisco Unified SRST 9.0, the values for the max-dn and timeouts busy commands were hardcoded for Cisco Unified 8941 and 8945 SCCP IP phones.

In Cisco Unified SRST 9.0, you can configure the max-dn and timeouts busy commands in call-manager-fallback configuration mode. Use the max-dn command to set the maximum number of DNs that can be supported by the router and enable dual-line mode, octo-line mode, or both modes. Use the timeouts busy command to set the timeout value for call transfers to busy destinations.

For configuration information, see the “Configuring the Maximum Number of Calls” section on page 160.

Cisco Unified 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones

In Cisco Unified SRST 9.0, the maximum number of calls for Cisco Unified 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP phones is controlled by the phones.

Prerequisites

- Cisco Unified SRST 9.0 and later versions.
- Correct firmware is installed:
Voice and Fax Support on Cisco ATA-187

Cisco ATA-187 is a SIP-based analog telephone adaptor that turns traditional telephone devices into IP devices. Cisco ATA-187 can connect with a regular analog FXS phone or fax machine on one end, while the other end is an IP side that uses SIP for signaling and registers as a Cisco Unified SIP IP phone.

Cisco ATA-187 functions as a Cisco Unified SIP IP phone that supports T.38 fax relay and fax pass-through, enabling the real-time transmission of fax over IP networks. The fax rate is from 7.2 to 14.4 kbps.

For information on feature support for the Cisco ATA-187 in Cisco Unified SRST, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

For more information on Cisco ATA-187, see Cisco ATA 187 Analog Telephone Adaptor Administration Guide for SIP.

New Features in Cisco Unified SRST Version 8.8

Cisco Unified SRST 8.8 supports the following new Cisco Unified SCCP IP phones:

- Cisco Unified 6945 SCCP IP Phones
- Cisco Unified 8941 SCCP IP Phones
- Cisco Unified 8945 SCCP IP Phones

Support for Cisco Unified 6945, 8941, and 8945 SCCP IP Phones

For information on feature support for the Cisco Unified 6945, 8941, and 8945 SCCP IP Phones in Cisco Unified SRST, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

For information on the Cisco Unified 6945 SCCP IP Phone, see Cisco Unified IP Phone 6945 User Guide for Cisco Unified Communications Manager Express Version 8.8 (SCCP).

For information on the Cisco Unified 8941 and 8945 SCCP IP Phones, see Cisco Unified IP Phone 8941 and 8945 User Guide for Cisco Unified Communications Manager Express Version 8.8 (SCCP).

New Features in Cisco Unified SRST Version 8.0

Beginning with Cisco IP Phone firmware 8.5(3) and Cisco IOS Release 15.1(1)T, Cisco SRST supports SIP signaling over UDP, TCP, and TLS connections, providing both RTP and SRTP media connections based on the security settings of the IP phone.

New Features in Cisco Unified SRST Version 7.0/4.3

Cisco Unified SRST 7.0/4.3 supports the following new features:
New Features in Cisco Unified SRST Version 4.2(1)

Cisco Unified SRST Version 4.2(1) introduces the following new features:
- Enhancements for Enhanced 911 Services, page 138

New Features in Cisco Unified SRST Version 4.1

Cisco Unified SRST Version 4.1 introduces the following new feature:
- Enhanced 911 Services, page 138

New Features in Cisco Unified SRST Version 4.0

Cisco Unified SRST Version 4.0 has introduced the following new features:
- Additional Cisco Unified IP Phone Support, page xxx
- Cisco IP Communicator Support, page xxxi
- Fax Pass-through using SCCP and ATAs Support, page xxxi
- H.323 VoIP Call Preservation Enhancements for WAN Link Failures for SCCP Phones, page xxxi
- Video Support, page xxxi

Additional Cisco Unified IP Phone Support

The following IP phones are supported with Cisco Unified SRST systems:
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G and Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7960G
- Cisco Unified IP Phone 7961G and Cisco Unified IP Phone 7961G-GE

In addition, the Cisco Unified IP Phone 7914 Expansion Module can attach to the Cisco 7941G-GE and Cisco 7961G-GE. The Cisco 7914 Expansion Module adds additional features, such as adding 14 line appearances or speed-dial numbers to your phone. You can attach one or two expansion modules to your IP phone. When you use two expansion modules, you have 28 additional line appearances or speed-dial numbers, or a total of 34 line appearances or speed-dial numbers. For more information, see Cisco IP Phone 7914 Expansion Module Quick Start Guide.

No additional SRST configuration is required for these phones.

The show ephone command is enhanced to display the configuration and status of the new Cisco IP Phones added to SRST Version 4.0. For more information, see the show ephone command in Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions).
To determine compatible firmware, platforms, memory, and additional voice products that are associated with Cisco Unified SRST 4.0, see Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products.

Cisco IP Communicator Support

Cisco IP Communicator is a software-based application that delivers enhanced telephony support on personal computers. This SCCP-based application allows computers to function as IP phones, providing high-quality voice calls on the road, in the office, or from wherever users may have access to the corporate network. Cisco IP Communicator appears on a user's computer monitor as a graphical, display-based IP phone with a color screen, a key pad, feature buttons, and soft keys.

Fax Pass-through using SCCP and ATAs Support

Fax pass-through mode is now supported using Cisco VG 224 voice gateways, Analog Telephone Adaptors (ATA), and SCCP. ATAs ship with SIP firmware, so SCCP firmware must be loaded before this feature can be used.

Note

For ATAs that are registered to a Cisco Unified SRST system to participate in FAX calls, they must have their ConnectMode parameter set to use the “standard payload type 0/8” as the RTP payload type in FAX pass-through mode. For ATAs used with Cisco Unified SRST 4.0 and higher versions, this is done by setting bit 2 of the ConnectMode parameter to 1 on the ATA. For more information, see the “Parameters and Defaults” chapter in Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP.

H.323 VoIP Call Preservation Enhancements for WAN Link Failures for SCCP Phones

H.323 VoIP call preservation enhancements for WAN link failures sustains connectivity for H.323 topologies where signaling is handled by an entity, such as Cisco Unified Communications Manager, that is different from the other endpoint and brokers signaling between the two connected parties. Call preservation is useful when a gateway and the other endpoint (typically a Cisco Unified IP phone) are collocated at the same site and the call agent is remote and therefore more likely to experience connectivity failures. H.323 VoIP call preservation enhancements does not support SIP Phones.

For configuration information see the “Configuring H.323 Gateways” chapter in Cisco IOS H.323 Configuration Guide.

Video Support

This feature allows you to set video parameters for the Cisco Unified SRST to maintain close feature parity with Cisco Unified CM. When the Cisco Unified SRST is enabled, Cisco Unified IP Phones do not have to be reconfigured for video capabilities because all ephones retain the same configuration used with Cisco Unified CM. However, you must enter call-manager-fallback configuration mode to set video parameters for Cisco Unified SRST. The feature set for video is the same as that for Cisco Unified SRST audio calls.
For more information, see the “Setting Video Parameters” section on page 355.

New Features in Cisco Unified SRST Version 3.4

Cisco SRST V3.4 introduced the new features described in the following section:

- Cisco SIP SRST 3.4, page xxxii

Cisco SIP SRST 3.4

Cisco SIP SRST Version 3.4 describes SRST functionality for Session Initiation Protocol (SIP) networks. Cisco SIP SRST Version 3.4 provides backup to an external SIP call control (IP-PBX) by providing basic registrar and back-to-back user agent (B2BUA) services. These services are used by a SIP IP phone in the event of a WAN connection outage when the SIP phone is unable to communicate with its primary SIP proxy.

Cisco SIP SRST Version 3.4 can support SIP phones with standard RFC 3261 feature support locally and across SIP WAN networks. With Cisco SIP SRST Version 3.4, SIP phones can place calls across SIP networks in the same way as Skinny Client Control Protocol (SCCP) phones. For full information about SIP SRST, Version 3.4, see Cisco SIP SRST Version 3.4 System Administrator Guide.

New Features in Cisco SRST Version 3.3

Cisco SRST V3.3 introduced the new features described in the following sections:

- Secure SRST, page xxxii
- Cisco Unified IP Phone 7970G and Cisco Unified 7971G-GE Support, page xxxiii
- Enhancement to the show ephone Command, page xxxiii

Secure SRST

Secure Cisco IP phones that are located at remote sites and that are attached to gateway routers can communicate securely with Cisco Unified Communications Manager using the WAN. But if the WAN link or Cisco Unified Communications Manager goes down, all communication through the remote phones becomes nonsecure. To overcome this situation, gateway routers can now function in secure SRST mode, which activates when the WAN link or Cisco Unified Communications Manager goes down. When the WAN link or Cisco Unified Communications Manager is restored, Cisco Unified Communications Manager resumes secure call-handling capabilities.

Secure SRST provides new SRST security features such as authentication, integrity, and media encryption. Authentication provides assurance to one party that another party is whom it claims to be. Integrity provides assurance that the given data has not been altered between the entities. Encryption implies confidentiality; that is, that no one can read the data except the intended recipient. These security features allow privacy for SRST voice calls and protect against voice security violations and identity theft. For more information see the “Configuring Secure SRST for SCCP and SIP” section on page 239.
Cisco Unified IP Phone 7970G and Cisco Unified 7971G-GE Support

The Cisco Unified IP Phones 7970G and 7971G-GE are full-featured telephones that provide voice communication over an IP network. They function much like a traditional analog telephones, allowing you to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more. In addition, because the phones are connected to your data network, they offer enhanced IP telephony features, including access to network information and services, and customizable features and services. The phones also support security features that include file authentication, device authentication, signaling encryption, and media encryption.

The Cisco Unified IP Phones 7970G and 7971G-GE also provide a color touchscreen, support for up to eight line or speed-dial numbers, context-sensitive online help for buttons and feature, and a variety of other sophisticated functions. No configurations specific to SRST are necessary.

For more information, see the Cisco Unified IP Phone 7900 Series documentation index.

Note
The Cisco Unified IP Phone 7914 Expansion Module can attach to your Cisco Unified IP Phones 7970G and 7971G-GE. See the “Cisco Unified IP Phone Expansion Module 7914 Support” section on page xliii for more information.

Enhancement to the show ephone Command

The show ephone command is enhanced to display the configuration and status of the Cisco Unified IP Phone 7970G and Cisco Unified IP Phone 7971G-GE. For more information, see the show ephone command in Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions).

New Features in Cisco SRST Version 3.2

Cisco SRST V3.2 introduced the new features described in the following sections:

- Enhancement to the alias Command, page xxxiii
- Enhancement to the cor Command, page xxxiv
- Enhancement to the pickup Command, page xxxiv
- Enhancement to the user-locale Command, page xxxiv
- Increased the Number of Cisco Unified IP Phones Supported on the Cisco 3845, page xxxiv
- MOH Live-Feed Support, page xxxiv
- No Timeout for Call Preservation, page xxxv
- RFC 2833 DTMF Relay Support, page xxxv
- Translation Profile Support, page xxxv

Enhancement to the alias Command

The alias command is enhanced as follows:

- The cfw keyword was added, providing call forward no-answer/busy capabilities.
New Features in Cisco SRST Version 3.2

- The maximum number of `alias` commands used for creating calls to telephone numbers that are unavailable during Cisco Unified Communications Manager fallback was increased to 50.
- The `alternate-number` argument can be used in multiple `alias` commands.

For more information, see the `alias` command in *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.

**Enhancement to the `cor` Command**

The maximum number of `cor` lists has increased to 20.

For more information, see the `cor` command in *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.

**Enhancement to the `pickup` Command**

The `pickup` command was introduced to enable the PickUp soft key on all Cisco Unified IP Phones, allowing an external Direct Inward Dialing (DID) call coming into one extension to be picked up from another extension during SRST.

For more information, see the `pickup` command in *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.

**Enhancement to the `user-locale` Command**

The `user-locale` command is enhanced to display the Japanese Katakana country code. Japanese Katakana is available in Cisco Unified Communications Manager V4.0 or later versions.

For more information, see the `user-locale` command in the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.

**Increased the Number of Cisco Unified IP Phones Supported on the Cisco 3845**

The Cisco 3845 now supports 720 phones and up to 960 ephone-dns or virtual voice ports.

**MOH Live-Feed Support**

Cisco Unified SRST is enhanced with the new `moh-live` command. The `moh-live` command provides live-feed MOH streams from an audio device connected to an E&M or FXO port to Cisco IP phones in SRST mode. If an FXO port is used for a live feed, the port must be supplied with an external third-party adaptor to provide a battery feed. Music from a live feed is obtained from a fixed source and is continuously fed into the MOH playout buffer instead of being read from a flash file. Live-feed MOH can also be multicast to Cisco IP phones. See the “Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource” section on page 11 for configuration instructions.
No Timeout for Call Preservation

To preserve existing H.323 calls on the branch in the event of an outage, disable the H.225 keepalive timer by entering the `no h225 timeout keepalive` command. This feature is supported in Cisco IOS Releases 12.3(7)T1 and higher versions. See the “Cisco Unified SRST Feature Overview” section on page 1 for more information.

H.323 is not supported with SIP phones.

RFC 2833 DTMF Relay Support

Cisco Skinny Client Control Protocol (SCCP) phones, such as those used with Cisco SRST systems, provide only out-of-band DTMF digit indications. To enable SCCP phones to send digit information to remote SIP-based IVR and voice-mail applications, Cisco SRST 3.2 and later versions provide conversion from the out-of-band SCCP digit indication to the SIP standard for DTMF relay, which is RFC 2833. You select this method in the SIP VoIP dial peer using the `dtmf-relay rtp-nte` command. See the “How to Configure DTMF Relay for SIP Applications and Voicemail” section on page 350 for configuration instructions.

To use voicemail on a SIP network that connects to a Cisco Unity Express system, use a nonstandard SIP Notify format. To configure the Notify format, use the `sip-notify` keyword with the `dtmf-relay` command. Using the `sip-notify` keyword may be required for backward compatibility with Cisco SRST Versions 3.0 and 3.1.

Translation Profile Support

Cisco SRST 3.2 and later versions support translation profiles. Translation profiles allow you to group translation rules together and to associate translation rules with the following:

- Called numbers
- Calling numbers
- Redirected called numbers

See the “Enabling Translation Profiles” section on page 200 for more configuration information. For more information on the `translation-profile` command, see Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions).

New Features in Cisco SRST Version 3.1

Cisco SRST V3.1 introduced the new features described in the following sections:

- [Cisco Unified IP Phone 7920 Support](page xxxvi)
- [Cisco Unified IP Phone 7936 Support](page xxxvi)

**Note**

For information about Cisco Unified IP phones, see the [Cisco Unified IP Phone 7900 Series documentation](#).
Cisco Unified IP Phone 7920 Support

The Cisco Unified Wireless IP Phone 7920 is an easy-to-use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco Unified CM and Cisco Aironet 1200, 1100, 350, and 340 Series of Wi-Fi (IEEE 802.11b) access points. As a key part of the Cisco AVVID Wireless Solution, the Cisco Unified Wireless IP Phone 7920 delivers seamless intelligent services, such as security, mobility, quality of service (QoS), and management, across an end-to-end Cisco network.

No configuration is necessary.

Cisco Unified IP Phone 7936 Support

The Cisco Unified IP Conference Station 7936 is an IP-based, hands-free conference room station that uses VoIP technology. The IP Conference Station replaces a traditional analog conferencing unit by providing business conferencing features—such as call hold, call resume, call transfer, call release, redial, mute, and conference—over an IP network.

No configuration is necessary.

New Features in Cisco SRST Version 3.0

Cisco SRST V3.0 introduced the new features described in the following sections:

- Additional Language Options for IP Phone Display, page xxxvi
- Consultative Call Transfer and Forward Using H.450.2 and H.450.3 for SCCP Phones, page xxxvii
- Customized System Message for Cisco Unified IP Phones, page xxxvii
- Dual-Line Mode, page xxxvii
- E1 R2 Signaling Support, page xxxviii
- European Date Formats, page xxxix
- Huntstop for Dual-Line Mode, page xxxix
- Music-on-Hold for Multicast from Flash Files, page xxxix
- Ringing Timeout Default, page xxxix
- Secondary Dial Tone, page xxxix
- Enhancement to the show ephone Command, page xl
- System Log Messages for Phone Registrations, page xl
- Three-Party G.711 Ad Hoc Conferencing, page xl
- Support for Cisco VG248 Analog Phone Gateway 1.2(1) and Higher Versions, page xl

Additional Language Options for IP Phone Display

Displays for the Cisco Unified IP Phone 7940G and Cisco Unified IP Phone 7960G can be configured with additional ISO-3166 codes for German, Danish, Spanish, French, Italian, Japanese, Dutch, Norwegian, Portuguese, Russian, Swedish, United States.
Consultative Call Transfer and Forward Using H.450.2 and H.450.3 for SCCP Phones

Cisco SRST V1.0, Cisco SRST V2.0, and Cisco SRST V2.1 allow blind call transfers and blind call forwarding. Blind calls do not give transferring and forwarding parties the ability to announce or consult with destination parties. These three versions of Cisco SRST use a Cisco SRST proprietary mechanism to perform blind transfers. Cisco SRST V3.0 adds the ability to perform call transfers with consultation using the ITU-T H.450.2 (H.450.2) standard and call forwarding using the ITU-T H.450.3 (H.450.3) standard for H.323 calls.

Cisco SRST V3.0 provides support for IP phones to initiate call transfer and forwarding with H.450.2 and H.450.3 by using the default session application. The built-in H.450.2 and H.450.3 support that is provided by the default session application applies to call transfers and call forwarding initiated by IP phones, regardless of the PSTN interface type.

Note: All voice gateway routers in the VoIP network must support H.450. For H.450 support, routers with Cisco SRST must run either Cisco SRST V3.0 and higher versions or Cisco IOS Release 12.2(15)ZJ and later releases. Routers without Cisco SRST must run either Cisco SRST V2.1 and higher versions or Cisco IOS Release 12.2(11)YT and later releases. SIP phones does not support this feature.

For more information about the default session application, see the Default Session Application Enhancements document.

For configuration information, see the “Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0” section on page 208.

Customized System Message for Cisco Unified IP Phones

The display message that appears on Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7940G, Cisco Unified IP Phone 7960G, and Cisco Unified IP Phone 7910 units when they are in fallback mode can be customized. The new system message command allows you to edit these display messages on a per-router basis. The custom system message feature supports English only.

For further information, see the “Configuring Customized System Messages for Cisco Unified IP Phones” section on page 154.

Dual-Line Mode

A new keyword that was added to the max-dn command allows you to set IP phones to dual-line mode. Each dual-line IP phone must have one voice port and two channels to handle two independent calls. This mode enables call waiting, call transfer, and conference functions on a single ephone-dn (ephone directory number). There is a maximum number of DNs available during Cisco SRST fallback. The max-dn command affects all IP phones on a Cisco SRST router.

For configuration information, see the “Configuring Dual-Line Phones” section on page 156.
E1 R2 Signaling Support

Cisco SRST V3.0 supports E1 R2 signaling. R2 signaling is an international signaling standard that is common to channelized E1 networks; however, there is no single signaling standard for R2. The ITU-T Q.400-Q.490 recommendation defines R2, but a number of countries and geographic regions implement R2 in entirely different ways. Cisco Systems addresses this challenge by supporting many localized implementations of R2 signaling in its Cisco IOS software.

The Cisco Systems E1 R2 signaling default is ITU, which supports the following countries: Denmark, Finland, Germany, Russia (ITU variant), Hong Kong (ITU variant), and South Africa (ITU variant). The expression “ITU variant” means there are multiple R2 signaling types in the specified country, but Cisco supports the ITU variant.

Cisco Systems also supports specific local variants of E1 R2 signaling in the following regions, countries, and corporations:

- Argentina
- Australia
- Bolivia
- Brazil
- Bulgaria
- China
- Colombia
- Costa Rica
- East Europe (includes Croatia, Russia, and Slovak Republic)
- Ecuador (ITU)
- Ecuador (LME)
- Greece
- Guatemala
- Hong Kong (uses the China variant)
- Indonesia
- Israel
- Korea
- Laos
- Malaysia
- Malta
- New Zealand
- Paraguay
- Peru
- Philippines
- Saudi Arabia
- Singapore
- South Africa (Panaftel variant)
- Telmex Corporation (Mexico)
- Telnor Corporation (Mexico)
- Thailand
- Uruguay
- Venezuela
- Vietnam

**European Date Formats**

The date format on Cisco IP phone displays can be configured with the following two additional formats:

- yy-mm-dd (year-month-day)
- yy-dd-mm (year-day-month)

For configuration information, see the “Configuring IP Phone Clock, Date, and Time Formats” section on page 150.

**Huntstop for Dual-Line Mode**

A new keyword was added to the `huntstop` command. The `channel` keyword causes hunting to skip the secondary channel in dual-line configuration if the primary line is busy or does not answer.

For configuration information, see the “Configuring Dial-Peer and Channel Hunting” section on page 204.

**Music-on-Hold for Multicast from Flash Files**

Cisco SRST can be configured to support continuous multicast output of MOH from a flash MOH file in flash memory.

For more information, see the “Defining XML API Schema” section on page 236.

**Ringing Timeout Default**

A ringing timeout default can be configured for extensions on which no-answer call forwarding has not been enabled. Expiration of the timeout causes incoming calls to return a disconnect code to the caller. This mechanism provides protection against hung calls for inbound calls received over interfaces such as Foreign Exchange Office (FXO) that do not have forward-disconnect supervision. For more information, see the “Configuring the Ringing Timeout Default” section on page 206.

**Secondary Dial Tone**

A secondary dial tone is available for Cisco Unified IP Phones running Cisco SRST. The secondary dial tone is generated when a user dials a predefined PSTN access prefix. An example would be the different dial tone heard when a designated number is pressed to reach an outside line.
The secondary dial tone is created through the secondary dialtone command. For more information, see the “Configuring a Secondary Dial Tone” section on page 155.

Enhancement to the show ephone Command

The show ephone command is enhanced to display the following:

- Configuration and status of additional phones (new keywords: 7905, 7914, 7935, ATA)
- Status of all phones with the call-forwarding all (CFA) feature enabled on at least one of their DNs (new keyword: cfa)

For more information, see the show ephone command in Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions).

System Log Messages for Phone Registrations

Diagnostic messages are added to the system log whenever a phone registers or unregisters from Cisco Unified SRST.

Three-Party G.711 Ad Hoc Conferencing

Cisco SRST supports three-party ad hoc conferencing using the G.711 coding technique. For conferencing to be available, an IP phone must have a minimum of two lines connected to one or more buttons.

For more information, see the “Enabling Three-Party G.711 Ad Hoc Conferencing” section on page 234.

Support for Cisco VG248 Analog Phone Gateway 1.2(1) and Higher Versions

The Cisco VG248 Analog Phone Gateway is a mixed-environment solution, enabled by Cisco AVVID (Architecture for Voice, Video and Integrated Data), that allows organizations to support their legacy analog devices while taking advantage of the new opportunities afforded through the use of IP telephony. The Cisco VG248 is a high-density gateway for using analog phones, fax machines, modems, voice-mail systems, and speakerphones within an enterprise voice system based on Cisco Unified CM.

During Cisco Unified CM fallback, Cisco SRST considers the Cisco VG248 to be a group of Cisco Unified IP Phones. Cisco Unified SRST counts each of the 48 ports on the Cisco VG248 as a separate Cisco Unified IP Phone. Support for Cisco VG248 Version 1.2(1) and higher versions is also available in Cisco Unified SRST Version 2.1.

For more information, see Cisco VG248 Analog Phone Gateway Data Sheet and Cisco VG248 Analog Phone Gateway Version 1.2(1) Release Notes.

New Features in Cisco SRST Version 2.1

Cisco SRST V2.1 introduced the new features described in the following sections:

- Additional Language Options for IP Phone Display, page xlii
- Cisco SRST Aggregation, page xlii
New Features in Cisco SRST Version 2.1

- Cisco ATA 186 and ATA 188 Support, page xlii
- Cisco Unified IP Phone 7902G Support, page xlii
- Cisco Unified IP Phone 7905G Support, page xliii
- Cisco Unified IP Phone 7912G Support, page xliii
Chapter iii Cisco Unified Survivable Remote Site Telephony Feature Roadmap

New Features in Cisco SRST Version 2.1

- Cisco Unified IP Phone Expansion Module 7914 Support, page xliii
- Enhancement to the dialplan-pattern Command, page xliii

Note
For information about Cisco Unified IP phones, see the Cisco Unified IP Phone 7900 Series documentation.

Additional Language Options for IP Phone Display

Displays for the Cisco Unified IP Phone 7940G and Cisco Unified IP Phone 7960G can be configured with ISO-3166 codes for the following countries:

- France
- Germany
- Italy
- Portugal
- Spain
- United States

Note
This feature is available only in Cisco Unified SRST running under Cisco Unified CM V3.2.

For configuration information, see the “Configuring IP Phone Language Display” section on page 152.

Cisco SRST Aggregation

For systems running Cisco Unified CM 3.3(2) and later versions, the restriction of running Cisco SRST on a default gateway was removed. Multiple SRST routers can be used to support additional phones. Note that dial peers and dial plans need to be carefully planned and configured for call transfer and forwarding to work properly.

Cisco ATA 186 and ATA 188 Support

The Cisco ATA analog telephone adaptors are handset-to-Ethernet adaptors that allow regular analog telephones to operate on IP-based telephony networks. Cisco ATAs support two voice ports, each with an independent telephone number. The Cisco ATA 188 also has an RJ-45 10/100BASE-T data port. Cisco SRST supports Cisco ATA 186 and Cisco ATA 188 using Skinny Client Control Protocol (SCCP) for voice calls only.

Cisco Unified IP Phone 7902G Support

The Cisco Unified IP Phone 7902G is an entry-level IP phone that addresses the voice communications needs of a lobby, laboratory, manufacturing floor, hallway, or other area where only basic calling capability is required.
The Cisco Unified IP Phone 7902G is a single-line IP phone with fixed feature keys that provide one-touch access to the redial, transfer, conference, and voice-mail access features. Consistent with other Cisco IP phones, the Cisco Unified IP Phone 7902G supports inline power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control and thus greater network availability.

**Cisco Unified IP Phone 7905G Support**

The Cisco Unified IP Phone 7905G is a basic IP phone that provides a core set of business features. It provides single-line access and four interactive soft keys that guide a user through call features and functions via the pixel-based liquid crystal display (LCD). The graphic capability of the display presents calling information, intuitive access to features, and language localization in future firmware releases. The Cisco Unified IP Phone 7905G supports inline power, which allows the phone to receive power over the LAN.

No configuration is necessary.

**Cisco Unified IP Phone 7912G Support**

The Cisco Unified IP Phone 7912G provides core business features and addresses the communication needs of a cubicle worker who conducts low to medium telephone traffic. Four dynamic soft keys provide access to call features and functions. The graphic display shows calling information and allows access to features.

The Cisco Unified IP Phone 7912G supports an integrated Ethernet switch, providing LAN connectivity to a local PC. In addition, the Cisco Unified IP Phone 7912G supports inline power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control and thus greater network availability. The combination of inline power and Ethernet switch support reduces cabling needs to a single wire to the desktop.

**Cisco Unified IP Phone Expansion Module 7914 Support**

The Cisco Unified IP Phone 7914 Expansion Module attaches to your Cisco Unified IP Phone 7960G, adding 14 line appearances or speed-dial numbers to your phone. You can attach one or two expansion modules to your IP phone. When you use two expansion modules, you have 28 additional line appearances or speed-dial numbers or a total of 34 line appearances or speed-dial numbers.

**Enhancement to the dialplan-pattern Command**

A new keyword was added to the `dialplan-pattern` command. The `extension-pattern` keyword sets an extension number’s leading digit pattern when it is different from the E.164 telephone number’s leading digits defined in the `pattern` variable. This enhancement allows manipulation of IP phone abbreviated extension number prefix digits. See the `dialplan-pattern` command in *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.
New Features in Cisco SRST Version 2.02

Cisco SRST Version 2.02 introduced the new features described in the following sections:

- Cisco Unified IP Phone Conference Station 7935 Support, page xliv
- Increase in Directory Numbers, page xliv
- Cisco Unity Voicemail Integration Using In-Band DTMF Signaling Across the PSTN and BRI/PRI, page xlv

Cisco Unified IP Phone Conference Station 7935 Support

The Cisco IP Conference Station 7935 is an IP-based, full-duplex hands-free conference station for use on desktops and offices and in small-to-medium-sized conference rooms. This device attaches a Cisco Catalyst 10/100 Ethernet switch port with a simple RJ-45 connection and dynamically configures itself to the IP network via the DHCP. Other than connecting the Cisco 7935 to an Ethernet switch port, no further administration is necessary. The Cisco 795 dynamically registers to Cisco Unified CM for connection services and receives the appropriate endpoint phone number and any software enhancements or personalized settings, which are preloaded within Cisco Unified CM.

The Cisco Unified IP Phone 7935 provides three soft keys and menu navigation keys that guide a user through call features and functions. The Cisco Unified IP Phone 7935 also features a pixel-based LCD display. The display provides features such as date and time, calling party name, calling party number, digits dialed, and feature and line status. No configuration is necessary.

Increase in Directory Numbers

Table iii-6 shows the increases in directory numbers.

<table>
<thead>
<tr>
<th>Cisco Router</th>
<th>Maximum Phones</th>
<th>Increase in Maximum Directory Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From</td>
<td>To</td>
</tr>
<tr>
<td>Cisco 1751</td>
<td>24</td>
<td>96</td>
</tr>
<tr>
<td>Cisco 1760</td>
<td>24</td>
<td>96</td>
</tr>
<tr>
<td>Cisco 2600XM</td>
<td>24</td>
<td>96</td>
</tr>
<tr>
<td>Cisco 2691</td>
<td>72</td>
<td>216</td>
</tr>
<tr>
<td>Cisco 3640</td>
<td>72</td>
<td>216</td>
</tr>
<tr>
<td>Cisco 3660</td>
<td>240</td>
<td>720</td>
</tr>
<tr>
<td>Cisco 3725</td>
<td>144</td>
<td>432</td>
</tr>
<tr>
<td>Cisco 3745</td>
<td>240</td>
<td>720</td>
</tr>
</tbody>
</table>
Cisco Unity Voicemail Integration Using In-Band DTMF Signaling Across the PSTN and BRI/PRI

Cisco Unity voicemail and other voicemail systems can be integrated with Unified SRST. Voicemail integration introduces six new commands:

- pattern direct
- pattern ext-to-ext busy
- pattern ext-to-ext no-answer
- pattern trunk-to-ext busy
- pattern trunk-to-ext no-answer
- vm-integration

Where to Go Next

Proceed to the “Setting Up the Network” section on page 123.
Cisco Unified SRST Feature Overview

This chapter describes Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) and what it does. It also includes information about support for Cisco Unified IP Phones and Platforms, specifications, features, prerequisites, restrictions and where to find additional reference documents.

For the most up-to-date information about Cisco Unified IP Phone support, the maximum number of Cisco Unified IP Phones, the maximum number of directory numbers (DNs) or virtual voice ports, and memory requirements for Cisco Unified SRST and Cisco Unified SIP SRST, see Cisco Unified SRST Supported Firmware, Platforms, Memory, and Voice Products.

Contents

- Cisco Unified SCCP SRST, page 1
- Cisco Unified SIP SRST, page 9
- Cisco Unified SRST Licenses
- Interface Support for Unified CME and Unified SRST, page 16
- MGCP Gateways and SRST, page 17
- Support for Cisco Unified IP Phones and Platforms, page 24
- IPv6 Support for Unified SRST SIP IP Phones, page 17
- Multicast Music On Hold, page 26
- Where to Go Next, page 29
- Additional References, page 29
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 32

Cisco Unified SCCP SRST

- Information About SCCP SRST, page 2
- Prerequisites for Configuring Cisco Unified SCCP SRST, page 4
- Restrictions for Configuring Cisco Unified SCCP SRST, page 7
Information About SCCP SRST

Cisco Unified SRST provides Cisco Unified CM with fallback support for Cisco Unified IP phones that are attached to a Cisco router on your local network. Cisco Unified SRST enables routers to provide call-handling support for Cisco Unified IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Unified CM installations or when the WAN connection is down.

Cisco Unified CM supports Cisco Unified IP phones at remote sites attached to Cisco multiscrvice routers across the WAN. Prior to Cisco Unified SRST, when the WAN connection between a router and the Cisco Unified CM failed or when connectivity with Cisco Unified CM was lost for some reason, Cisco Unified IP phones on the network became unusable for the duration of the failure. Cisco Unified SRST overcomes this problem and ensures that the Cisco Unified IP phones offer continuous (although minimal) service by providing call-handling support for Cisco Unified IP phones directly from the Cisco Unified SRST router. The system automatically detects a failure and uses Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch office router to provide call processing for Cisco Unified IP phones that are registered with the router. When the WAN link or connection to the primary Cisco Unified CM is restored, call handling reverts back to the primary Cisco Unified CM.

When Cisco Unified IP phones lose contact with primary, secondary, and tertiary Cisco Unified CM, they must establish a connection to a local Cisco Unified SRST router to sustain the call-processing capability necessary to place and receive calls. The Cisco Unified IP phone retains the IP address of the local Cisco Unified SRST router as a default router in the Network Configuration area of the Settings menu. The Settings menu supports a maximum of five default router entries; however, Cisco Unified CM accommodates a maximum of three entries. When a secondary Cisco Unified CM is not available on the network, the local Cisco Unified SRST Router's IP address is retained as the standby connection for Cisco Unified CM during normal operation.

Note: Cisco Unified CM fallback mode telephone service is available only to those Cisco Unified IP phones that are supported by a Cisco Unified SRST router. Other Cisco Unified IP phones on the network remain out of service until they re-establish a connection with their primary, secondary, or tertiary Cisco Unified CM.

Typically, it takes three times the keepalive period for a phone to discover that its connection to Cisco Unified CM has failed. The default keepalive period is 30 seconds. If the phone has an active standby connection established with a Cisco Unified SRST router, the fallback process takes 10 to 20 seconds after connection with Cisco Unified CM is lost. An active standby connection to a Cisco Unified SRST router exists only if the phone has the location of a single Cisco Unified CM in its Unified Communications Manager list. Otherwise, the phone activates a standby connection to its secondary Cisco Unified CM.

Note: The time it takes for a Cisco Unified IP Phone to fallback to the SRST router can vary depending on the phone type. Phones such as the Cisco 7902, Cisco 7905, and Cisco 7912 can take approximately 2.5 minutes to fallback to SRST mode.

If a Cisco Unified IP phone has multiple Cisco Unified CM in its Cisco Unified CM list, it progresses through its list of secondary and tertiary Cisco Unified CM before attempting to connect with its local Cisco Unified SRST router. Therefore, the time that passes before the Cisco Unified IP phone eventually establishes a connection with the Cisco Unified SRST router increases with each attempt to contact to a Cisco Unified CM. Assuming that each attempt to connect to a Cisco Unified CM takes about 1 minute, the Cisco Unified IP phone in question could remain offline for 3 minutes or more following a WAN link failure.
Note

During a WAN connection failure, when Cisco Unified SRST is enabled, Cisco Unified IP phones display a message informing you that they are operating in Cisco Unified CM fallback mode. For example, the Cisco Unified IP Phone 7960G and Cisco Unified IP Phone 7940G display a "CM Fallback Service Operating" message, and the Cisco Unified IP Phone 7910 displays a "CM Fallback Service" message when operating in Cisco Unified CM fallback mode. When the Cisco Unified CM is restored, the message goes away and full Cisco Unified IP phone functionality is restored.

While in Cisco Unified CM fallback mode, Cisco Unified IP phones periodically attempt to re-establish a connection with Cisco Unified CM at the central office. Generally, the default time that Cisco Unified IP phones wait before attempting to re-establish a connection to a remote Cisco Unified CM is 120 seconds. The time can be changed in Cisco Unified CM; see the "Device Pool Configuration Settings" chapter in the appropriate Cisco Unified CM Administration Guide. A manual reboot can immediately reconnect Cisco Unified IP phones to Cisco Unified CM.

When a connection is re-established with Cisco Unified CM, Cisco Unified IP phones automatically cancel their registration with the Cisco Unified SRST Router. However, if a WAN link is unstable, Cisco Unified IP phones can bounce between Cisco Unified CM and Cisco Unified SRST. A Cisco Unified IP phone cannot re-establish a connection with the primary Cisco Unified CM at the central office if it is currently engaged in an active call.

Cisco Unified SRST supports the following call combinations:

- SCCP phone to SCCP phone
- SCCP phone to PSTN/router voice-port
- SCCP phone to WAN VoIP using SIP or H.323
- SIP phone to SIP phone
- SIP phone to PSTN / router voice-port
- SIP phone to Skinny Client Control Protocol (SCCP) phone
- SIP phone to WAN VoIP using SIP

Figure 1-1 shows a branch office with several Cisco Unified IP phones connected to a Cisco Unified SRST router. The router provides connections to both a WAN link and the PSTN. Typically, the Cisco Unified IP phones connect to their primary Cisco Unified Communications Manager at the central office via the WAN link. When the WAN connection is down, the Cisco Unified IP phones use the Cisco Unified SRST router as a fallback for their primary Cisco Unified Communications Manager. The branch office Cisco Unified IP phones are connected to the PSTN through the Cisco Unified SRST router and are able to make and receive off-net calls.
On H.323 gateways for SCCP SRST, when the WAN link fails, active calls from Cisco Unified IP phones to the PSTN are not maintained by default. Call preservation may work with the `no h225 timeout keepalive` command.

Under default configuration, the H.323 gateway maintains a keepalive signal with Cisco Unified Communications Manager and terminates H.323-to-PSTN calls if the keepalive signal fails, for example, if the WAN link fails. To disable this behavior and help preserve existing calls from local Cisco Unified IP phones, you can use the `no h225 timeout keepalive` command. Disabling the keepalive mechanism only affects calls that will be torn down as a result of the loss of the H.225 keepalive signal. For information regarding disconnecting a call when an inactive condition is detected, see the *Media Inactive Call Detection* document.

**Prerequisites for Configuring Cisco Unified SCCP SRST**

Before configuring Cisco Unified SRST, you must do the following:

- An SRST feature license is required to enable the Cisco Unified SCCP SRST feature. Contact your account representative if you have further questions. For more information about Licensing on Unified SRST, refer to *Cisco Unified SRST Licenses*, page 12.
- You have an account on Cisco.com to download software.

To obtain an account on Cisco.com, go to [www.cisco.com](http://www.cisco.com) and click *Register* at the top of the screen.
Installing Cisco Unified Communications Manager

When installing Cisco Unified Communications Manager, consider the following:

- See the installation instructions for your version in the *Cisco Unified Communications Manager Install and Upgrade Guides*.
- Integrate Cisco Unified SRST with Cisco Unified Communications Manager. Integration is performed from Cisco Unified Communications Manager. See the “Integrating Cisco Unified SCCP SRST with Cisco Unified Communications Manager” section on page 5.

Installing Cisco Unified SCCP SRST

Cisco Unified SRST versions have different installation instructions:

- Installing Cisco Unified SRST V3.0 and Later Versions, page 5
- Installing Cisco Unified SRST V2.0 and V2.1, page 5
- Installing Cisco Unified SRST V1.0, page 5

To update Cisco Unified SRST, follow the installation instructions described in this section.

Installing Cisco Unified SRST V3.0 and Later Versions

Install the Cisco IOS software release image containing the Cisco SRST or Cisco Unified SRST version that is compatible with your Cisco Unified Communications Manager version. See the “Cisco Unified Communications Manager Compatibility” section on page 26. Cisco IOS software can be downloaded from the Cisco Software Center at [http://www.cisco.com/public/sw-center/](http://www.cisco.com/public/sw-center/).

Cisco SRST and Cisco Unified SRST can be configured to support continuous multicast output of music-on-hold (MOH) from a flash MOH file in flash memory. For more information, see the “Defining XML API Schema” section on page 236. If you plan to use MOH, go to the Technical Support Software Download site at [http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp](http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp) and copy the music-on-hold.au file to the flash memory on your Cisco SRST or Cisco Unified SRST router.

Installing Cisco Unified SRST V2.0 and V2.1


Installing Cisco Unified SRST V1.0

Cisco SRST V1.0 runs with Cisco Communications Manager V3.0.5 only. It is recommended that you upgrade to the latest Cisco Unified Communications Manager and Cisco Unified SRST versions.

Integrating Cisco Unified SCCP SRST with Cisco Unified Communications Manager

There are two procedures for integrating Cisco Unified SRST with Cisco Unified Communications Manager. Procedure selection depends on the Cisco Unified Communications Manager version that you have.

If You Have Cisco Communications Manager V3.3 or Later Versions

If you have Cisco Communications Manager V3.3 or later versions, you must create an SRST reference and apply it to a device pool. An SRST reference is the IP address of the Cisco Unified SRST Router.
Step 1 Create an SRST reference.
   a. From any page in Cisco Unified Communications Manager, click System and SRST.
   b. On the Find and List SRST References page, click Add a New SRST Reference.
   c. On the SRST Reference Configuration page, enter a name in the SRST Reference Name field and the IP address of the Cisco SRST router in the IP Address field.
   d. Click Insert.

Step 2 Apply the SRST reference or the default gateway to one or more device pools.
   a. From any page in Cisco Unified Communications Manager, click System and Device Pool.
   b. On the Device Pool Configuration page, click on the required device pool icon.
   c. On the Device Pool Configuration page, choose an SRST reference or “Use Default Gateway” from the SRST Reference field’s menu.

If You Have Cisco Unified Communications Manager Version Prior to V3.3

If you have firmware versions that enable Cisco Unified SRST by default, no additional configuration is required on Cisco Unified Communications Manager to support Cisco Unified SRST. If your firmware versions disable Cisco Unified SRST by default, you must enable Cisco Unified SRST for each phone configuration.

Step 1 Go to the Cisco Unified Communications Manager Phone Configuration page.
   a. From any page in Cisco Unified Communications Manager, click Device and Phone.
   b. In the Find and List Phones page, click Find.
   c. After a list of phones appears, click on the required device name.
   d. The Phone Configuration appears.

Step 2 In the Phone Configuration page, go to the Product Specific Configuration section at the end of the page, choose Enabled from the Cisco Unified SRST field’s menu, and click Update.

Step 3 Go to the Phone Configuration page for the next phone and choose Enabled from the Cisco Unified SRST field’s menu by repeating Step 1 and Step 2.
Restrictions for Configuring Cisco Unified SCCP SRST

Table 1-1 provides a history of restrictions from Cisco SCCP SRST Version 1.0 to the present version of Cisco Unified SCCP SRST.

### Table 1-1  Restrictions from Cisco SCCP SRST from the Present Version to Version 1.0

<table>
<thead>
<tr>
<th>Cisco Unified SRST Version</th>
<th>Cisco IOS Release</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| Version 4.1                | 12.4.(15)T        | • Enhanced 911 Services for Cisco Unified SRST does not interface with the Cisco Emergency Responder.  
• The information about the most recent phone that called 911 is not preserved after a reboot of Cisco Unified SRST.  
• Cisco Emergency Responder does not have access to any updates made to the emergency call history table when remote IP phones are in Cisco Unified SRST fallback mode. Therefore, if the PSAP calls back after the Cisco Unified IP phones register back to Cisco Unified Communications Manager, Cisco Emergency Responder will not have any history of those calls. As a result, those calls will not get routed to the original 911 caller. Instead, the calls are routed to the default destination that is configured on Cisco Emergency Responder for the corresponding ELIN.  
• For Cisco Unified Wireless IP Phone 7920 and 7921, a caller’s location can only be determined by the static information configured by the system administrator. For more information, see the Precautions for Mobile Phones in Configuring Enhanced 911 Services.  
• The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL).  
• Using ELINs for multiple purposes can result in unexpected interactions with existing Cisco Unified SRST features. These multiple uses of an ELIN can include configuring an ELIN for use as an actual phone number (ephone-dn, voice register dn, or FXS destination-pattern), a Call Pickup number, or an alias rerouting number. For more information, see the Multiple Usages of an ELIN in Configuring Enhanced 911 Services.  
• There are a number of other ways that your configuration of Enhanced 911 Services can interact with existing Cisco Unified SRST features and cause unexpected behavior. For a complete description of interactions between Enhanced 911 Services and existing Cisco Unified SRST features, see the Interactions with Existing Cisco Unified CME Features in Configuring Enhanced 911 Services. |
## Table 1-1 Restrictions from Cisco SCCP SRST from the Present Version to Version 1.0 (continued)

<table>
<thead>
<tr>
<th>Cisco Unified SRST Version</th>
<th>Cisco IOS Release</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 4.0</td>
<td>12.4(4)XC</td>
<td>• All of the restrictions in Cisco SRST Version 1.0.</td>
</tr>
<tr>
<td>Version 3.4</td>
<td>12.4(4)T</td>
<td>• Caller-id display on supported Cisco Unified IP phones: SIP phones in fallback mode displays the name and number of the caller. SCCP phones in fallback mode display only the caller-id number assigned to the line; the caller-ID name configuration for SCCP phones is not preserved during SRST fallback.</td>
</tr>
<tr>
<td>Version 3.2</td>
<td>12.3(11)T</td>
<td>• Call transfer is supported only on the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– VoIP H.323, VoFR, and VoATM between Cisco gateways running Cisco IOS Release 12.2(11)T and using the H.323 nonstandard information element</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– FXO and FXS loop-start (analog)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– FXO and FXS ground-start (analog)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Ear and mouth (E&amp;M) (analog) and DID (analog)</td>
</tr>
<tr>
<td>Version 3.1</td>
<td>12.3(7)T</td>
<td>– T1 channel-associated signaling (CAS) with FXO and FXS ground-start signaling</td>
</tr>
<tr>
<td>Version 3.0</td>
<td>12.2(15)ZJ, 12.3(4)T</td>
<td>– T1 CAS with E&amp;M signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– All PRI and BRI switch types</td>
</tr>
<tr>
<td>Version 2.1</td>
<td>12.2(15)T</td>
<td>• The following Cisco Unified IP Phone function keys are dimmed because they are not supported during SRST operation:</td>
</tr>
<tr>
<td>Version 2.02</td>
<td>12.2(13)T</td>
<td>– MeetMe</td>
</tr>
<tr>
<td>Version 2.01</td>
<td>12.2(11)T</td>
<td>– GPickUp (group pickup)</td>
</tr>
<tr>
<td>Version 2.0</td>
<td>12.2(8)T, 12.2(8)T1</td>
<td>– Park</td>
</tr>
<tr>
<td></td>
<td>12.2(2)XT</td>
<td>– Confrn (conference)</td>
</tr>
<tr>
<td>Version 1.0</td>
<td>12.2(2)XB</td>
<td>• Although the Cisco IAD2420 series integrated access devices (IADs) support the Cisco Unified SRST feature, this feature is not recommended as a solution for enterprise branch offices.</td>
</tr>
<tr>
<td></td>
<td>12.2(2)XG</td>
<td>• Does not support first generation Cisco Unified IP phones, such as Cisco IP Phone 30 VIP and Cisco IP Phone 12 SP+.</td>
</tr>
<tr>
<td></td>
<td>12.1(5)YD</td>
<td>• Does not support other Cisco Unified Communications Manager applications or services: Cisco IP SoftPhone, Cisco One: Voice and Unified Messaging Application, or Cisco IP Contact Center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does not support Centralized Automatic Message Accounting (CAMA) trunks on the Cisco 3660 routers.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>If you are in one of the states in the United States of America where there is a regulatory requirement for CAMA trunks to interface to 911 emergency services, and you would like to connect more than 48 Cisco Unified IP phones to the Cisco 3660 multiservice routers in your network, contact your local Cisco account team for help in understanding and meeting the CAMA regulatory requirements.</td>
</tr>
</tbody>
</table>
Cisco Unified SIP SRST

- Information About SIP SRST, page 9
- Prerequisites for Configuring Cisco Unified SIP SRST, page 9
- Restrictions for Configuring Cisco Unified SIP SRST, page 10

Information About SIP SRST

This guide describes Cisco Unified SRST functionality for SIP networks. Cisco Unified SIP SRST provides backup to an external SIP call control (IP-PBX) by providing basic registrar and redirect server or back-to-back user agent (B2BUA) services. These services are used by a SIP IP phone in the event of a WAN connection outage when the SIP phone is unable to communicate with its primary SIP proxy.

Cisco Unified SIP SRST can support SIP phones with standard RFC 3261 feature support locally and across SIP WAN networks. With Cisco Unified SIP SRST, SIP phones can place calls across SIP networks in the same way as SCCP phones.

Cisco Unified SIP SRST supports the following call combinations:

- SIP phone to SIP phone
- SIP phone to PSTN / router voice-port
- SIP phone to Skinny Client Control Protocol (SCCP) phone
- SIP phone to WAN VoIP using SIP

SIP proxy, registrar, and B2BUA servers are key components of a SIP VoIP network. These servers are usually located in the core of a VoIP network. If SIP phones located at remote sites at the edge of the VoIP network lose connectivity to the network core (because of a WAN outage), they may be unable to make or receive calls. Cisco Unified SIP SRST functionality on a SIP PSTN gateway provides service reliability for SIP-based IP phones in the event of a WAN outage. Cisco Unified SIP SRST enables the SIP IP phones to continue to make and receive calls to and from the PSTN and also to make and receive calls to and from other SIP IP phones.

To see a branch office Cisco Unified IP Phones connected to a remote central Cisco Unified CM Operating in SRST mode, see Figure 1-1.

Prerequisites for Configuring Cisco Unified SIP SRST

Before configuring Cisco Unified SIP SRST, you must do the following:

- An SRST feature license is required to enable the Cisco Unified SIP SRST feature. Contact your account representative if you have further questions. For more information about Licensing on Unified SRST, refer Cisco Unified SRST Licenses, page 12.
Restrictions for Configuring Cisco Unified SIP SRST

Table 1-2 provides a history of restrictions from Cisco SIP SRST Version 3.0 to the present version of Cisco Unified SIP SRST.

Table 1-2  Restrictions from Cisco SIP SRST from the Present Version to Version 3.0

<table>
<thead>
<tr>
<th>Cisco Unified SRST Version</th>
<th>Cisco IOS Release</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8.0</td>
<td>15.1(1)T</td>
<td>- SIP phones may be configured on the Cisco Unified CM with an Authenticated device security mode. The Cisco Unified CM ensures integrity and authentication for the phone using a TLS connection with NULL-SHA cipher for signaling. If such an Authenticated SIP phone fails over to the Cisco Unified SRST device, and if the Cisco Unified CM and SRST device are configured to support secure SIP SRST, it will register using TCP instead of TLS/TCP, thus disabling the Authenticated mode until the phone fails back to the Cisco Unified CM.</td>
</tr>
</tbody>
</table>
Table 1-2 Restrictions from Cisco SIP SRST from the Present Version to Version 3.0 (continued)

<table>
<thead>
<tr>
<th>Cisco Unified SRST Version</th>
<th>Cisco IOS Release</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| Version 4.1               | 12.4.(15)T        | • Cisco Unified SRST does not support BLF speed-dial notification, call forward all synchronization, dial plans, directory services, or music-on-hold (MOH).  
• Prior to SIP phone load 8.0, SIP phones maintained dual registration with both Cisco Unified Communications Manager and Cisco Unified SRST simultaneously. In SIP phone load 8.0 and later versions, SIP phones use keepalive to maintain a connection with Cisco Unified SRST during active registration with Cisco Unified Communications Manager. Every two minutes, a SIP phone sends a keepalive message to Cisco Unified SRST. Cisco Unified SRST responds to this keepalive with a 404 message. This process repeats until fallback to Cisco Unified SRST occurs. After fallback, SIP phones send a keepalive message every two minutes to Cisco Unified Communications Manager while the phones are registered with Cisco Unified SRST. Cisco Unified SRST continues to support dual registration for SIP phone loads older than 8.0.  
• Enhanced 911 Services for Cisco Unified SRST does not interface with the Cisco Emergency Responder.  
• The information about the most recent phone that called 911 is not preserved after a reboot of Cisco Unified SRST.  
• Cisco Emergency Responder does not have access to any updates made to the emergency call history table when remote IP Phones are in Cisco Unified SRST fallback mode. Therefore, if the PSAP calls back after the Cisco Unified IP Phones register back to Cisco Unified Communications Manager, Cisco Emergency Responder will not have any history of those calls. As a result, those calls will not get routed to the original 911 caller. Instead, the calls are routed to the default destination that is configured on Cisco Emergency Responder for the corresponding ELIN.  
• For Cisco Unified Wireless 7920 and 7921 IP Phones, a caller’s location can only be determined by the static information configured by the system administrator. For more information, see Precautions for Mobile Phones in Configuring Enhanced 911 Services.  
• The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL).  
• Using ELINs for multiple purposes can result in unexpected interactions with existing Cisco Unified SRST features. These multiple uses of an ELIN can include configuring an ELIN for use as an actual phone number (ephone-dn, voice register dn, or FXS destination-pattern), a Call Pickup number, or an alias rerouting number. For more information, see Multiple Usages of an ELIN in Configuring Enhanced 911 Services.  
• There are a number of other ways that your configuration of Enhanced 911 Services can interact with existing Cisco Unified SRST features and cause unexpected behavior. For a complete description of interactions between Enhanced 911 Services and existing Cisco Unified SRST features, see the Interactions with Existing Cisco Unified CME Features in Configuring Enhanced 911 Services..
Cisco Unified SRST Licenses

You should purchase a Cisco Unified SRST license that entitle you to use Unified SRST. You can purchase:

Version 4.0
Version 3.4
Version 3.2
Version 3.1
Version 3.0
12.4(4)XC
12.4(4)T
12.3(11)T
12.3(7)T
12.2(15)ZJ
12.3(4)T

Not Supported

- MOH is not supported for a call hold invoked from a SIP phone. A caller hears only silence when placed on hold by a SIP phone.
- As of Cisco IOS Release 12.4(4)T, bridged call appearance, find-me, incoming call screening, paging, SIP presence, call park, call pickup, and SIP location are not supported.
- SIP-NAT is not supported.
- Cisco Unity Express is not supported.
- Transcoding is not supported.

Phone Features

- For call waiting to work on the Cisco ATA and Cisco IP Phone 7912 and Cisco Unified IP Phone 7905G with a 1.0(2) build, the incoming call leg should be configured with the G.711 codec.

Note

Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7912G, and Cisco Analog Telephone Adaptor (ATA) 186 are not capable of dual registration; thus they are not supported and have limited functionality with Cisco Unified SIP SRST.

General

- Call detail records (CDRs) are only supported by standard IOS RADIUS support; CDRs are not supported otherwise.
- All calls must use the same codec, either G.729r8 or G.711.
- Calls that have been transferred cannot be transferred a second time.
- URL dialing is not supported. Only number dialing is supported.
- The SIP registrar functionality provided by Cisco Unified SIP SRST provides no security or authentication services.
- SIP IP phones that do not support dual concurrent registration with both their primary and their backup SIP proxy or registrar may be unable to receive incoming calls from the Cisco Unified SIP SRST gateway during a WAN outage. These phones may take a significant amount of time to discover that their primary SIP proxy or registrar is unreachable before they initiate a fallback registration to their backup proxy or registrar (the SIP SRST gateway).
- SIP-phone-to-SIP-trunk support requires Refer and 302/300 Redirection to be supported by the SIP trunk (Version 3.0).

Table 1-2 Restrictions from Cisco SIP SRST from the Present Version to Version 3.0 (continued)
Cisco Unified SRST Feature Overview

Chapter 1

Cisco Unified SRST Licenses

- Cisco Unified SRST Permanent License
- Cisco Smart License

Cisco Unified SRST Permanent License

When you purchase a Cisco Unified SRST permanent license, the permanent license is installed on the device when the product is shipped to you. A permanent license never expires and you will gain access to that particular feature set for the lifetime of the device across all IOS release. If you purchase a permanent license for Cisco Unified SRST, you do not have to go through the Evaluation Right to Use and Right To Use (RTU) licensing processes for using the features. If you want to purchase a CME-SRST license for your existing device, you have to go through the RTU licensing process for using the features. There is no change in the existing process for purchasing the license.

The Cisco Unified SRST permanent license is available in the form of an XML cme-locked3 file. You should get the XML file and load it in the flash memory of the device. To install the permanent license from the command prompt, use the `license install flash0:cme-locked3` command. The `cme-locked3` is the xml file of the license.

Cisco Smart License

From Release 12.1 onwards, Unified SRST supports Smart Licensing, apart from the existing CSL licensing model. Smart Licensing is supported only on Cisco 4000 Series Integrated Services Router. Depending on the technology package available on the router, licenses such as UCK9 and Security are supported using Smart Licensing.

Smart Software Licensing is Cisco's new licensing model that gives you visibility into license ownership and consumption. Smart licenses can be managed by a cloud-based deployment model, namely Cisco Smart Software Manager (CSSM) or an on-prem software, Smart Software Manager satellite. Unified SRST is supported by both CSSM and satellite. Your access to the customer Smart Account residing on CSSM is authenticated using valid Cisco credentials. With the Smart Licensing support for Unified SRST, your device can register with CSSM or Cisco Smart Software Manager satellite. You can access your Licenses at the Cisco Software Central.

Unified SRST needs to register with CSSM or Cisco Smart Software Manager satellite to report license consumption. You can register Unified SRST to a Virtual Account within a Smart Account by generating a token ID from it, and pasting it to the underlying platform, Cisco 4000 Series Integrated Services Router. Once the token is generated, it can be used to register many other product instances in your network.

On the Unified SRST router, you need to ensure that the call home feature is not disabled. Also, Smart Licensing should be enabled at the router using the CLI command `license smart enable`. Use the `no` form of the command to disable Smart Licensing.

For more information on configuring Smart Licensing in your router, see Cisco 4000 Series ISRs Software Configuration Guide. For more information on configuring Call Home for your devices, see Configure Call Home, page 15. Once Smart Licensing is enabled, the router enters a 90-day evaluation period that persist until it registers to CSSM or the Cisco Smart Software Manager satellite.

You can register the router to CSSM or Cisco Smart Software Manager satellite with the token ID. To register the device (Unified SRST router) with CSSM or Cisco Smart Software Manager satellite, use the CLI command `license smart register idtoken`. For information on registering the device with CSSM, see Device Registration, Software Activation Configuration Guide, Cisco IOS Release 15M&T.
Upon successful registration, Unified SRST is in Registered status. As part of the registration process, the router sends an authorization request, indicating the number of phone endpoints defined by the `max-pool`, for SIP SRST, and `max-ephone`, for SCCP SRST. Based on the licenses in the Smart Account, CSSM or Cisco Smart Software Manager satellite responds with one of the defined statuses such as Authorized (using less than or equal to the number of licenses provisioned in CSSM or Cisco Smart Software Manager satellite) or Out-of-Compliance (using more than it has licenses for).

The license limit on Unified SRST is restricted by the maximum platform limit defined for the Unified SRST router (a cumulative sum of phones configured under `max-pool` and `max-ephone`). Hence, the license usage count cannot exceed the platform limit set for the Unified SRST router even when the cumulative sum of phones configured under `max-pool` and `max-ephone` exceeds the defined platform limit. For more details on the platform limits defined for Unified SRST, see Cisco Unified SRST/E-SRST 12.1 Supported Firmware, Platforms, Memory, and Voice Products.

CSSM or Smart Software Manager satellite reports license consumption submitted by the platform in its User Interface (UI), and subtracts it from the available licenses in the Virtual Account within the Smart Account. Unified SRST supports only one license entitlement to validate phones configured on Unified SRST.

**Note**

The SRST_EP license count reflects the total phone count of both the ephones and pools that are configured in the Unified SRST irrespective of whether the phones are registered or not.

Unified SRST sends an authorization request when a license consumption changes or every 30 days to let CSSM or Cisco Smart Software Manager satellite know it's still available and communicating. The ID certificate issued to identify Unified SRST at time of registration is valid for one year, and is automatically renewed every six months.

**Note**

If the router does not communicate with CSSM or Cisco Smart Software Manager satellite for a period of 90 days, the license authorization expires. When the license authorization expires, the devices registered on Unified SRST change status to Out of Compliance.

The license count is evaluated for the number of phones configured across the routers. The CSSM Licenses page reflects the total license count usage, the total number of licenses available for a type of license (Quantity), number of licenses currently used (In Use), and the number of unused or over-used licenses (Surplus/Shortage). If you do not have enough Cisco Smart licenses, you are in Out-of-Compliance state.

For example, consider a smart account in CSSM with 50 SRST_EP licenses. If the user has a registered Unified SRST with 20 phones configured, the CSSM licenses page reflects Quantity as 50, In Use as 20, and Surplus as 30. For more information on Smart Software Manager, see Cisco Smart Software Manager User Guide.

For more information on switching between CSL and Cisco Smart License, see Licensing Modes, page 16.

The license entitlement for Unified SRST smart license is displayed on the router as follows:

```
Router# show license summary
Smart Licensing is ENABLED
Registration:
  Status: REGISTERED
  Smart Account: ABC
  Virtual Account: XYZ
```
Configure Call Home

To configure the call home destination address and proxy server details for the HTTP proxy request, perform the following steps.

Prerequisites

- Cisco Smart Software Licensing is enabled.

SUMMARY STEPS

1. configure terminal
2. call-home destination address http url
3. call-home http-proxy proxy_address port port number
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router# configure terminal
```

<table>
<thead>
<tr>
<th><strong>Step 2</strong> call-home destination address http url</th>
<th>(Optional) Defines the destination URL to which Call Home messages, including licensing requests are sent. The destination URL can be the URL for Transport Gateway or CSSM satellite. The URL to the Cisco Smart Licensing production server is set by default.</th>
</tr>
</thead>
</table>
| Example: 
```
Router(config)# call-home destination address http http://10.22.183.117:8080/ddce/services/DDCEService
```

License Authorization:
Status: AUTHORIZED
Last Communication Attempt: SUCCESS
Next Communication Attempt: Apr 13 07:11:48 2017 UTC

License Usage:

<table>
<thead>
<tr>
<th>License</th>
<th>Entitlement tag</th>
<th>Count</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>regid.2014-12.com.ci...</td>
<td>(ISR_4351_UnifiedCommun..)</td>
<td>1</td>
<td>AUTHORIZED</td>
</tr>
<tr>
<td>regid.2016-10.com.ci...</td>
<td>(SRST_EP)</td>
<td>4</td>
<td>AUTHORIZED</td>
</tr>
</tbody>
</table>

Export-Controlled Functionality: Not Allowed
Last Renewal Attempt: None
Next Renewal Attempt: Jun 07 12:08:10 2017 UTC
Chapter 1 Cisco Unified SRST Feature Overview

Interface Support for Unified CME and Unified SRST

From Unified SRST 12.1 onwards, both CSL and Smart Licensing modes are supported. That is, customers can continue with CSL by not enabling Smart Licensing. Alternatively, they can enable Smart Licensing and decide later to go back to CSL by disabling Smart Licensing with the `no license smart enable` command. When you switch to CSL from the Smart Licensing mode, you need to ensure that the End User License Agreement (EULA) is signed. CSL is not supported unless the EULA is signed. Use the CLI command `license accept end user agreement` in global configuration mode to configure EULA.

To verify the status of the license issued to phones registered on Unified SRST, you can use the `show license` command.

```
Router# show license?
  all   Show license all information
  status Show license status information
  summary Show license summary
  tech   Show license tech support information
  udi    Show license udi information
  usage  Show license usage information
```

Restrictions

- For the Unified SRST license, the UCK9 technology package must be available if the Collaboration Professional Suite package is not installed.

To purchase a license, go to [http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key](http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key). To activate cme-srst feature license, see the Activating CME-SRST Feature License document.

Interface Support for Unified CME and Unified SRST

Unified CME and Unified SRST routers have multiple interfaces that are used for signaling and data packet transfers. The two types of interfaces available on a Cisco router include the physical interface and the virtual interface. The types of physical interfaces available on a router depends on its interface processors or port adapters. Virtual interfaces are software-based interfaces that you create in the memory of the networking device using Cisco IOS commands. When you need to configure a virtual interface for connectivity, you can use the Loopback Interface for Unified CME and Unified SRST.

The following interfaces are supported on Unified CME and Unified SRST:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>call-home http-proxy proxy_address port port number</code></td>
<td>(Optional) Specifies the proxy server for the HTTP request.</td>
</tr>
</tbody>
</table>

Example:

```
Router(config)# call-home http-proxy 7.7.7.7 port 3218
```

Step 4 `end`

Example:

```
Router(config)# end
```

Exits to privileged EXEC mode.

---

Licensing Modes

To verify the status of the license issued to phones registered on Unified SRST, you can use the `show license` command.

```
Router# show license?
  all   Show license all information
  status Show license status information
  summary Show license summary
  tech   Show license tech support information
  udi    Show license udi information
  usage  Show license usage information
```
MGCP Gateways and SRST

MGCP fallback is a different feature than SRST and, when configured as an individual feature, can be used by a PSTN gateway. To use SRST as your fallback mode on an MGCP gateway, SRST and MGCP fallback must both be configured on the same gateway. MGCP and SRST have had the capability to be configured on the same gateway since Cisco IOS Release 12.2(11)T.

To make outbound calls while in SRST mode on your MGCP gateway, two fallback commands must be configured on the MGCP gateway. These two commands allow SRST to assume control over the voice port and over call processing on the MGCP gateway. With Cisco IOS earlier than 12.3(14)T, the two commands are the `ccm-manager fallback-mgcp` and `call application alternate` commands. With Cisco IOS releases after 12.3(14)T, the `ccm-manager fallback-mgcp` and `service` commands must be configured. A complete configuration for these commands is shown in the section the “Enabling Cisco Unified SRST on an MGCP Gateway” section on page 124.

Note

The commands listed above are ineffective unless both commands are configured. For instance, your configuration will not work if you only configure the `ccm-manager fallback-mgcp` command.

For more information on the fallback methods for MGCP gateways, see the Configuring MGCP Gateway Support for Cisco Unified Communications Manager document or the MGCP Gateway Fallback Transition to Default H.323 Session Application document.

IPv6 Support for Unified SRST SIP IP Phones

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP). IPv6 uses packets to exchange data, voice, and video traffic over digital networks. Also, IPv6 increases the number of network address bits from 32 bits in IPv4 to 128 bits. From Unified SRST Release 12.0 onwards, Unified SRST supports IPv6 protocols for SIP IP phones.

IPv6 support in Unified SRST allows the network to behave transparently in a dual-stack (IPv4 and IPv6) environment and provides additional IP address space to SIP IP phones that are connected to the network. If you do not have a dual-stack configuration, configure the CLI command `call service stop` under `voice service voip` configuration mode before changing to dual-stack mode. For an example of switching to dual-stack mode, see Examples for Configuring IPv6 Pools for SIP IP Phones, page 23.

The Cisco IP Phone 7800 Series and 8800 Series are supported on IPv6 for Unified SRST.

For more information on configuring SIP IP phones for IPv6 source address, see Configure IPv6 Pools for SIP IP Phones, page 18.

For an example of configuring IPv6 Support on Unified SRST, see Examples for Configuring IPv6 Pools for SIP IP Phones, page 23.

Feature Support for IPv6 in Unified SRST SIP IP Phones

The following basic features are supported for a IPv6 WAN down scenario:
- Basic SIP Line (IPv4 or IPv6) to SIP Line calls (IPv4 or IPv6) when Unified SRST is in dual-stack **no anat** mode.

The following supplementary services are supported as part of IPv6 in Unified SRST IP Phones:
- Hold/Resume
- Call Forward
- Call Transfer
- Three-way Conference (with BIB conferencing only)
- Line to T1/E1 Trunk and Trunk to Line with Supplementary Service Features
- Fax to and from PSTN (IPv4 ATA to ISDN T1/E1) for both T.38 Fax Relay and Fax Passthrough

Restrictions

The following are the known restrictions for IPv6 support on Unified SRST:
- SIP Trunks are not supported on Unified SRST for IPv6 deployment. PSTN calls are supported only through T1/E1 trunks.
- SCCP IP Phones are not supported in a deployment of IPv6 for Unified SRST.
- SIP Phones can be either in IPv4 only or IPv6 only mode (**no anat**).
- Trancoding and Transrating are not supported.
- H.323 trunks are not supported.
- Secure SIP lines or trunks are not supported.
- IPv6 on Unified SRST is not supported on the Cisco IOS platform. The support is restricted to Cisco IOS XE platform with Cisco IOS Release 16.6.1 or later versions.

Configure IPv6 Pools for SIP IP Phones

**Before You Begin**
- Unified SRST 12.0 or a later version.
- IPv6 option only appears if protocol mode is dual-stack configured under sip-ua configuration mode or IPv6.
- Cisco Unified SRST License must be configured for the gateway to function as a Unified SRST gateway to support IPv6 functionality. For more information on licenses, see Cisco Unified SRST Licenses, page 12.
- Cisco Unified Communications Manager (Unified Communications Manager) is provisioned with the IPv6 address of Unified SRST. For information on configuration of Unified SRST on Unified Communications Manager, see the section **Survivable Remote Site Telephony Configuration** in Cisco Unified Communications Manager Administration Guide.
SUMMARY STEPS

5. enable
6. configure terminal
7. ipv6 unicast-routing
8. voice service voip
9. sip
10. no anat
11. call service stop
12. exit
13. exit
14. sip-ua
15. protocol mode {ipv4 | ipv6 | dual-stack [preference {ipv4 | ipv6}]}
16. exit
17. voice service {voip}
18. sip
19. no call service stop
20. exit
21. voice register global
22. default mode
23. max-dn max-directory-numbers
24. max-pool max-voice-register-pools
25. exit
26. voice register pool pool-tag
27. id { network address mask | ip address mask | mac address }
28. end
### IPv6 Support for Unified SRST SIP IP Phones

#### 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><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&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><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router #configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 unicast-routing</td>
<td>Enables the forwarding of IPv6 unicast datagrams.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>voice service voip</td>
<td>Enters voice-service configuration mode to specify a voice encapsulation type.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router (config)# voice service voip</td>
<td>voip—Specifies Voice over IP (VoIP) parameters.</td>
</tr>
<tr>
<td>Step 5</td>
<td>sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>no anat</td>
<td>Disables Alternative Network Address Types (ANAT) on a SIP trunk.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-serv-sip)# no anat</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>call service stop</td>
<td>Shuts down SIP call service.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-serv-sip)# call service stop</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>exit</td>
<td>Exits SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-serv-sip)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>Exits voice service voip configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voi-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# sip-ua</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>protocol mode {ipv4</td>
<td>ipv6</td>
</tr>
</tbody>
</table>
| Example: | Router(config-sip-ua)# protocol mode dual-stack preference ipv6 | - ipv4—Allows you to set the protocol mode as an IPv4 address.  
- ipv6—Allows you to set the protocol mode as an IPv6 address.  
- dual-stack—Allows you to set the protocol mode for both IPv4 and IPv6 addresses.  
- preference—Allows you to choose a preferred IP address family if protocol mode is dual-stack. |

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-sip-ua)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|         | voice service {voip} | Enters voice-service configuration mode to specify a voice encapsulation type.  
- voip—Specifies Voice over IP (VoIP) parameters. |
| Example: | Router(config)# voice service voip | |

<table>
<thead>
<tr>
<th>Step 14</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voi-serv)# sip</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 15</th>
<th>no call service stop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-serv-sip)# call service stop</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Activates SIP call service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-serv-sip)# exit</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Exits SIP configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 17</th>
<th>voice register global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config)# voice register global</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 18</th>
<th>default mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-register-global)# default mode</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Enables mode for provisioning SIP phones in Unified SRST. The default mode is Unified SRST itself.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 19</th>
<th>max-dn max-directory-numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-register-global)# max-dn 50</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Limits number of directory numbers to be supported by this router.</td>
</tr>
<tr>
<td>- Maximum number is platform and version-specific. Type ? for value.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 20</th>
<th>max-pool max-voice-register-pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-register-global)# max-pool 40</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Sets maximum number of SIP phones to be supported by the Unified SRST router.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 21</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config-register-global)# exit</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Exits voice register global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 22</th>
<th>voice register pool pool-tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>Router(config)# voice register pool 1</code></td>
</tr>
<tr>
<td>Purpose:</td>
<td>Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.</td>
</tr>
</tbody>
</table>
IPv6 Support for Unified SRST SIP IP Phones

Examples for Configuring IPv6 Pools for SIP IP Phones

The following example provides configuration of IPv6 pools for SIP IP Phones:

```
ipv6 unicast-routing
voice service voip
sip
no anat
call service stop
exit
exit
sip-ua
protocol mode dual-stack
exit
voice service voip
sip
no call service stop
exit
voice register global
default mode
max-dn 50
max-pool 40
exit
voice register pool 1
id network 2001:420:54FF:13::901:0/117
end
```

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>`id { network address mask mask</td>
<td>ip address mask mask</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-register-pool)# id network 2001:420:54FF:13::901:0/117</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-register-pool)# id network 10.64.88.0 mask 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td><code>end</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
The following example provides interface configuration for IPv6 supported on Unified SRST:

```
configure terminal
interface GigabitEthernet0/0/1
  ip address 10.64.86.229 255.255.255.0
  negotiation auto
  ipv6 address 2001:420:54FF:13::312:82/119
  ipv6 enable
```

The following example provides IP route configuration for IPv6 supported on Unified SRST:

```
```

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

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

The following example displays output when SIP call service is active with the `no call service stop` CLI command:

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

---

**Support for Cisco Unified IP Phones and Platforms**

The following sections provide information about Cisco Feature Navigator and the histories of Cisco Unified IP Phone, platform, and Cisco Unified CM support from Cisco SRST Version 1.0 to the present version of Cisco Unified SRST.

- Finding Cisco IOS Software Releases That Support Cisco Unified SRST, page 24
- Cisco Unified IP Phone Support, page 25
- Platform and Memory Support, page 25
- Cisco Unified Communications Manager Compatibility, page 26
- Signal Support, page 26
- Language Support, page 26
- Switch Support, page 26

---

**Finding Cisco IOS Software Releases That Support Cisco Unified SRST**

*Note*  
With Cisco IOS Release 12.4(15)T, the number of SIP phones supported on each platform is now equivalent to the number of SCCP phones supported. For example, 3845 now supports 720 phones regardless of whether these are SIP or SCCP.
To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.


### Cisco Unified IP Phone Support

For the most up-to-date information about Cisco Unified IP Phone support, see Compatibility Information.

For ATAs that are registered to a Cisco Unified SRST system to participate in FAX calls, they must have their ConnectMode parameter set to use the "standard payload type 0/8" as the RTP payload type in FAX passthrough mode. For ATAs used with Cisco Unified SRST 4.0 and higher versions, this is done by setting bit 2 of the ConnectMode parameter to 1 on the ATA. For more information, see the Parameters and Defaults chapter in Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP.

During Cisco Unified CM fallback, Cisco Unified SRST considers the Cisco VG248 to be a group of Cisco Unified IP phones. Cisco Unified SRST counts each of the 48 ports on the Cisco VG248 as a separate Cisco Unified IP phone. Support for Cisco VG248 Version 1.2(1) and higher versions is available as of Cisco SRST Version 2.1. For more information, see Cisco VG248 Analog Phone Gateway Data Sheet and Cisco VG248 Analog Phone Gateway Version 1.2(1) Release Notes.

For IPv6 Support on Unified SRST, all the legacy IP Phones and Voice Gateways must be converted or reconfigured to IPv4-Only SIP signaling from SCCP signaling, if applicable.

### Platform and Memory Support

For the most up-to-date information about Platform and Memory Support, see Compatibility Information.

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, see the online release notes or, if supported, Cisco Feature Navigator.

For the most up-to-date information about Cisco IOS software images, see Compatibility Information.
Cisco Unified Communications Manager Compatibility

See *Cisco Unified Communications Manager Compatibility Matrix.*

Signal Support

Cisco Unified SRST supports FXS, FXO, T1, E1, and E1 R2 signals.

Language Support

See *Cisco Unified Communications Manager Express Cisco Unified CME Localization Matrix.*

Switch Support

Cisco SRST 3.2 and later versions support all PRI and BRI switches including the following:

- basic-1tr6
- basic-5ess
- basic-dms100
- basic-net3
- basic-ni
- basic-ntt NTT switch type for Japan
- basic-ts013
- primary-4ess Lucent 4ESS switch type for the United States
- primary-5ess Lucent 5ESS switch type for the United States
- primary-dms100 Northern Telecom DMS-100 switch type for the United States
- primary-net5 NET5 switch type for the United Kingdom, Europe, Asia, and Australia
- primary-ni National ISDN switch type for the United States
- primary-ntt NTT switch type for Japan
- primary-qsig QSIG switch type
- primary-ts014 TS014 switch type for Australia (obsolete)

Multicast Music On Hold

For Unified SRST 3.0 and later versions, you can configure the MOH audio stream as a multicast source. A Unified SRST router that is configured for multicast MOH also transmits the audio stream on the physical IP interfaces of the specified router to permit access to the stream by external devices. Certain IP phones do not support multicast MOH because they do not support IP multicast. You can disable multicast MOH to individual phones that do not support multicast. Callers hear a repeating tone when they are placed on hold.
Multicast MOH on Unified SRST is supported for both SIP and SCCP phones. Support is offered for G.711 and G.729 codecs with multicast MOH on Unified SRST. Multicast MOH is supported on Cisco Integrated Services Router Generation 2 (ISR G2) and the Cisco 4000 Series Integrated Services Routers.

For SIP phones to play the Multicast MOH, you need to configure the CLI command `moh enable-g711 filename` (for example, `moh enable-g711 "flash:en_bacd_music_on_hold.au"` or `moh g729 flash:SampleAudioSource.g729.wav`). For SCCP phones to play Multicast MOH, you need to configure the CLI command `multicast moh ip-address port port-number [route ip-address-list]` (for example, `multicast moh 239.1.1.1 port 2000`), apart from the CLI command `moh filename`. If both the CLI commands are not configured, SCCP phones will only play tone on hold.

For more information on supporting Multicast MOH with Unified SRST for a scenario where WAN is available, see Information About Using Cisco Unified SRST Gateways as a Multicast MOH Resource, page 13.

**Configure Multicast Music On Hold for Unified SRST**

To configure multicast MOH for Unified SRST, perform the following steps.

**Prerequisites**
- Unified SRST 3.0 or later versions.
- IP phones do not support multicast at 224.x.x.x addresses.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. call-manager-fallback
4. moh filename
5. multicast moh ip-address port port-number [route ip-address-list]
6. 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:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 1  Cisco Unified SRST Feature Overview

#### Multicast Music On Hold

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4**

  `moh filename`

**Example:**

Router(config-cm-fallback)# moh enable-g711
`flash:en_bacd_music_on_hold.au`

OR

Router(config-cm-fallback)# moh g729
`flash:SampleAudioSource.g729.wav`

Enables music on hold using the specified file.
- If you specify a file with this command and later want to use a different file, you must disable use of the first file with the `no moh` command before configuring the second file.

| **Step 5**

  `multicast moh ip-address port port-number [route ip-address-list]`

**Example:**

Router(config-cm-fallback)# multicast moh 239.1.1.1
`port 2000`

Specifies that this audio stream is to be used for multicast and also for MOH.

**Note**
- This command is required to use MOH for internal calls and it must be configured after MOH is enabled with the `moh` command.

- `ip-address`—Destination IP address for multicast.

- `port port-number`—Media port for multicast.
  Range is 2000 to 65535. We recommend port 2000 because it is already used for normal RTP media transmissions between IP phones and the router.

**Note**
- Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.)

- `route`—(Optional) List of explicit router interfaces for the IP multicast packets.

- `ip-address-list`—(Optional) List of up to four explicit routes for multicast MOH. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the `ip source-address` command.

**Note**
- For MOH on internal calls, packet flow must be enabled to the subnet on which the phones are located.

| **Step 6**

  `exit`

**Example:**

Router(config-cm-fallback)# exit

Exits call-manager-fallback configuration mode.
Where to Go Next

The next chapters of this book describe how to configure Cisco Unified SIP SRST. As shown in Table 1-3, each chapter takes you through tasks in the order in which they need to be performed. The first task for configuring Cisco Unified SRST is to ensure that the basic software and hardware in your system are configured correctly for Cisco Unified SRST.

<table>
<thead>
<tr>
<th>Task</th>
<th>Where Task Is Described</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Setting up a Cisco Unified SRST system to communicate with your network</td>
<td>Setting Up the Network, page 123</td>
</tr>
<tr>
<td>8. Configuring Version 4.1 features</td>
<td>Cisco Unified SIP SRST 4.1, page 135</td>
</tr>
<tr>
<td>9. Setting up the basic Cisco Unified SRST phone configuration using SCCP</td>
<td>Setting Up Cisco Unified IP Phones using SCCP, page 145</td>
</tr>
<tr>
<td>10. Providing a backup to an external SIP call control (IP-PBX) by supplying basic registrar services</td>
<td>Setting Up Cisco Unified IP Phones using SIP, page 165</td>
</tr>
<tr>
<td>11. Configuring incoming and outgoing calls</td>
<td>Configuring Call Handling, page 183</td>
</tr>
<tr>
<td>12. Configuring optional security for SRST</td>
<td>Configuring Secure SRST for SCCP and SIP, page 239</td>
</tr>
<tr>
<td>13. Setting up voicemail</td>
<td>Integrating Voicemail with Cisco Unified SRST, page 331</td>
</tr>
<tr>
<td>14. Setting up video parameters</td>
<td>Setting Video Parameters, page 355</td>
</tr>
</tbody>
</table>

Additional References

The following sections provide additional references related to Cisco Unified SIP SRST:

- Related Documents, page 30
- Standards, page 32
- MIBs, page 32
- RFCs, page 32
- Technical Assistance, page 32
## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Documents</th>
</tr>
</thead>
</table>
| Cisco IOS voice product configuration | • Cisco IOS Voice Configuration Library  
  • Cisco IOS Voice Command Reference  
  • Cisco IOS Debug Command Reference  
  • Cisco IOS Tcl IVR and VoiceXML Application Guide  
  • Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide |
| Configuring SRST and MGCP Fallback | • Configuring MGCP Gateway Support for Cisco Unified Communications Manager  
  • MGCP Gateway Fallback Transition to Default H.323 Session Application  
  • Configuring SRS Telephony and MGCP Fallback |
| Cisco Unified Communications Manager user documentation | • Cisco Unified Communications Manager  
  • Cisco Unified Communications Manager Security Guide  
  • Cisco Unified Communications Operating System Administration Guide |
| Cisco Unified IP Phones | • Cisco 7900 Series Unified IP Phones End-User Guides  
  • Cisco IP Phone Authentication and Encryption for Cisco Communications Manager  
| Cisco Unified SRST commands and specifications | • Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)  
  • Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products  
  • Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products |
| Cisco Security Documentation | • Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways  
  • Cisco IOS Certificate Server  
  • Manual Certificate Enrollment (TFTP and Cut-and-Paste)  
  • Certification Authority Interoperability Commands  
  • Certificate Enrollment Enhancements |
<p>| Cisco SIP SRST V3.4: Cisco IOS SIP Survivable Remote Site Telephony Feature Roadmap | • Cisco IOS SIP SRST Feature Roadmap |
| Cisco SIP functionality | • Cisco IOS SIP Configuration Guide |</p>
<table>
<thead>
<tr>
<th><strong>Related Topic</strong></th>
<th><strong>Documents</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SRST command reference</td>
<td>• <em>Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference</em></td>
</tr>
<tr>
<td>Command reference information for voice</td>
<td>• <em>Cisco IOS Voice Command Reference</em></td>
</tr>
<tr>
<td>and telephony commands</td>
<td>• <em>Cisco IOS Debug Command Reference</em></td>
</tr>
<tr>
<td>DHCP</td>
<td>• <em>Cisco IOS DHCP Server</em></td>
</tr>
<tr>
<td>Media Inactive Call Detection</td>
<td>• <em>Media Inactive Call Detection</em></td>
</tr>
<tr>
<td>Phone documentation for Cisco Unified</td>
<td>• <em>Cisco Unified IP Phones 7900 Series</em></td>
</tr>
<tr>
<td>SRST</td>
<td>• <em>Survivable Remote Site Telephony</em></td>
</tr>
<tr>
<td>Standard Glossary</td>
<td>• <em>Cisco IOS Voice Configuration Library Glossary</em></td>
</tr>
<tr>
<td>Standard Preface</td>
<td>• <em>Cisco IOS Voice Configuration Library Preface</em></td>
</tr>
</tbody>
</table>
### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITU X. 509 Version 3</td>
<td>Public-Key and Attribute Certificate Frameworks</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS 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>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2246</td>
<td>The Transport Layer Security (TLS) Protocol Version 1.0</td>
</tr>
<tr>
<td>RFC 2543</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
<tr>
<td>RFC 3261</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
<tr>
<td>RFC 3711</td>
<td>The Secure Real-Time Transport Protocol (SRTP)</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support &amp; Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>

### Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at [http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html](http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html).
Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

This chapter describes the support for Unified SIP SRST on the Cisco 4000 Series Integrated Services platform.

Note
Unified SRST 12.6 on Cisco IOS XE Gibraltar 16.11.1a Release is not a recommended release version for call flows that include Multicast Music On Hold.

Contents

- Overview, page 34
- Platform and Memory Support, page 34
- Cisco IOS Software Releases that Support Unified SRST, page 34
- Feature Support, page 36
- Unified IP Phone Support, page 37
- Cisco Unified Communications Manager Compatibility, page 38
- Supported PSTN Trunk Connectivity, page 38
- Language Support, page 39
- Switch Support, page 39
- Interface Support for Unified SRST, page 39
- Simple Network Management Protocol (SNMP) Support for Unified SRST, page 40
- Licensing, page 40
- Configure SIP Registrar Functionality for SIP Phones on Unified SRST, page 44
- Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy, page 57
- Toll Fraud Prevention for SIP Line Side on Unified SRST, page 60
- IPv6 Support for Unified SRST SIP IP Phones, page 67
- Configure Unified SRST on Cisco 4000 Series Integrated Services Platform, page 73
- Configure Voice Hunt Groups on Unified SRST, page 77
- Configure Feature Support on Unified SIP SRST, page 80
Overview

This chapter describes Unified SRST functionality on Cisco 4000 Series Integrated Services Routers for SIP phones. Unified SIP SRST provides backup to Unified Communications Manager when the IP connectivity to Unified Communications Manager is down.

Cisco Unified SIP SRST supports the following during a WAN outage:

- Basic Registration of SIP phones.
- Basic call support on SIP phones.
- Basic supplementary services such as Call Transfer, MOH, and Conference
- SIP phone to SIP phone
- SIP phone to PSTN / router voice-port
- SIP phone to Skinny Client Control Protocol (SCCP) phone
- SIP phone to WAN VoIP using SIP

Platform and Memory Support

From Unified SRST Release 10.0 (Cisco IOS Release 15.3(3)M), Unified SIP SRST is supported on the Cisco 4000 Series Integrated Services platform. As part of the Cisco IOS Release 15.3(3)M Release, support was introduced on the Cisco 4451-X Integrated Services Router. From Unified SRST Release 10.5 (Cisco IOS Release 15.4(3)M, 15.4(3)S), SIP SRST is supported on all Cisco 4000 Series Integrated Services Routers.

The following Cisco 4000 Series Integrated Services Router platforms are supported:

- Cisco ISR 4321 Integrated Services Routers
- Cisco ISR 4331 Integrated Services Routers
- Cisco ISR 4351 Integrated Services Routers
- Cisco ISR 4431 Integrated Services Routers
- Cisco ISR 4451 Integrated Services Routers

For more information on Platform and Memory Support, see Compatibility Information.

Cisco IOS Software Releases that Support Unified SRST

For information on the Unified SRST Release and the corresponding IOS Software, see Unified CME, Unified SRST, and Cisco IOS Software Version Compatibility Matrix for related compatibility information.
To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Install Cisco IOS Software

To verify that the recommended software is installed on the Cisco router and if necessary, download and install a Cisco IOS Voice or higher image, perform the following steps.

Before You Begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware, and other optional hardware.

SUMMARY STEPS

1. Identify which Cisco IOS software release is installed on router.
2. Determine whether the Cisco IOS release supports the recommended Unified SRST.
3. Download and extract the recommended Cisco IOS IP Voice or higher image to flash memory.
4. Use the `reload` command to reload the Unified SRST router with the new software.

DETAILED STEPS

Step 1  Identify which Cisco IOS software release is installed on router. Log in to the router and use the `show version` EXEC command.

Example:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.3 T Software (C2600-I-MZ), Version 12.3(11)T, RELEASE SOFTWARE
```

Step 2  Compare the Cisco IOS release installed on the Cisco router to the information in the Cisco Unified CME, Unified SRST, and Cisco IOS Software Version Compatibility Matrix to determine whether the Cisco IOS release supports the recommended Unified SRST.

Step 3  If necessary, download and extract the recommended Cisco IOS IP Voice or higher image to flash memory in the router.


Step 4  To reload the Unified SRST router with the new software after replacing or upgrading the Cisco IOS release, use the `reload` privileged EXEC command.

Example:

```
Router# reload

System configuration has been modified. Save [yes/no]: Y
Building configuration...
OK
Proceed with reload? Confirm.
11w2d: %Sys-5-RELOAD: Reload requested by console. Reload reason: reload command
```
Feature Support

The following features are known to be supported for Unified SIP SRST on Cisco 4000 Series Integrated Services Platform:

- Auto-answer (If enabled on Unified Communications Manager)
- Alert/Semi-Consult/Attended/Consult Transfer
- Ad-hoc Software Conference
- Hold or Resume
- Headset Answer
- Caller ID Display
- Call Forward to Voice Hunt Group
- Call Transfer to a Voice Hunt Group
- Voicemail
- Message Waiting Indicator (MWI)
- Do Not Disturb (DND)
- DTMF
- Feature Button or Programmable Line Key (PLK) - If enabled on Unified Communications Manager
- Key Expansion Module (KEM - Supported only on the 8851/8851NR/8861 phones)
- Bulk Registration Support
- Enabling or Disabling KPML
- Alias Feature
- Call Forward (All, Busy, No Answer, Mailbox)
- Call Forward All Softkey on Phone
- Unicast MOH
- Audio codecs (G.722, G.711, G.729, iLBC)
- Translation Profile
- Conference Blocking
- Transfer Blocking
- COR
- Voice Class Codec
- SNMP/MIB (Supported only to get mode and number of registered phones)
Chapter 2  Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Unified IP Phone Support

Unified SIP SRST on Cisco 4000 Series Integrated Services Platform is supported on the following phone series:

- Cisco IP Phone 7800 Series
- Cisco IP Phone 8800 Series

For IPv6 Support on Unified SRST, all the legacy IP Phones and Voice Gateways must be converted or reconfigured to IPv4-Only SIP signaling from SCCP signaling, if applicable.

Restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers

- Multicast MOH for SIP is not supported on the Cisco 4000 Series Integrated Services Routers.
- Transcoding is not supported on the Unified SRST.
- Multi-VRF is not supported on the Cisco 4000 Series Integrated Services Routers for both SIP and SCCP SRST.
- Multi-VRF is supported only on the Cisco Integrated Services Routers Generation 2 (ISR G2). Voice VRF is not supported for SCCP SRST on Cisco Integrated Services Router Generation 2 (ISR G2).
- Shared lines and Mixed shared lines are not supported on the Unified SRST (supported on the Unified E-SRST).
- Privacy (on hold) is not supported on the Unified SRST (supported on the Unified E-SRST).
- SNMP/MIB support is restricted to fetching information on mode and number of registered phones.
- Unified SRST supports only the basic voice hunt group features. To configure advanced voice hunt group features, you must deploy the Cisco Unified Enhanced Survivable Remote Site Telephony.
- Video Calling is not supported on Unified SIP SRST.
- The existing support for Cisco Jabber is now End of Life (EOL). Hence, Cisco Jabber is not supported on Unified SRST, E-SRST or Secure SRST.
Cisco Unified Communications Manager Compatibility

For more information on Unified Communications Manager compatibility, see *Cisco Unified Communications Manager Compatibility Matrix*.

Installing Cisco Unified Communications Manager

When installing Cisco Unified Communications Manager, consider the following:

- See the installation instructions for your version in the *Cisco Unified Communications Manager Install and Upgrade Guides*.
- Integrate Cisco Unified SRST with Cisco Unified Communications Manager. Integration is performed from Cisco Unified Communications Manager. See the

Integrating Cisco Unified SIP SRST with Cisco Unified Communications Manager

The procedure for integrating Unified SRST with Cisco Unified Communications Manager is as follows:

For Cisco Communications Manager integration with Unified SIP SRST, you must create an SRST reference and apply it to a device pool. An SRST reference is the IP address of the Cisco Unified SRST Router.

**Step 1** Create an SRST reference.

a. From any page in Cisco Unified Communications Manager, click **System** and **SRST**.

b. On the Find and List SRST References page, click **Add a New SRST Reference**.

c. On the SRST Reference Configuration page, enter a name in the SRST Reference Name field and the IP address of the Cisco SRST router in the IP Address field.

d. Click **Insert**.

**Step 2** Apply the SRST reference or the default gateway to one or more device pools.

a. From any page in Cisco Unified Communications Manager, click **System** and **Device Pool**.

b. On the Device Pool Configuration page, click the required device pool icon.

c. On the Device Pool Configuration page, choose an SRST reference or “Use Default Gateway” from the SRST Reference field’s menu.

Supported PSTN Trunk Connectivity

Unified SRST is supported on SIP trunks. Also, Unified SIP SRST supports the following trunk types:

- FXO/FXS
- Basic Rate ISDN
- Primary Rate ISDN (T1 or E1)
Language Support

For information on language support, see *Localization Matrix*.

Switch Support

Unified SRST supports all PRI and BRI switches including the following:

- basic-1tr6
- basic-5ess
- basic-dms100
- basic-net3
- basic-ni
- basic-ntt NTT switch type for Japan
- basic-ts013
- primary-4ess Lucent 4ESS switch type for the United States
- primary-5ess Lucent 5ESS switch type for the United States
- primary-dms100 Northern Telecom DMS-100 switch type for the United States
- primary-net5 NET5 switch type for the United Kingdom, Europe, Asia, and Australia
- primary-ni National ISDN switch type for the United States
- primary-ntt NTT switch type for Japan
- primary-qsig QSIG switch type
- primary-ts014 TS014 switch type for Australia (obsolete)

Interface Support for Unified SRST

Unified SRST routers have multiple interfaces that are used for signaling and data packet transfers. The two types of interfaces available on a Cisco router include the physical interface and the virtual interface. The type of physical interfaces available on a router depends on its interface processors or port adapters. Virtual interfaces are software-based interfaces that you create in the memory of the networking device using Cisco IOS commands. To configure a virtual interface for connectivity, you can use the Loopback Interface for Unified SRST.

The following interfaces are supported on Unified SRST:

- Gigabit Ethernet Interface (IEEE 802.3z) (*interface gigabitethernet*)
- Loopback Interface (*interface loopback*)
- Fast Ethernet Interface (*interface fastethernet*)
Simple Network Management Protocol (SNMP) Support for Unified SRST

Unified SRST supports Simple Network Management Protocol (SNMP) Management Information Base (MIBs) for monitoring the product status. Unified SRST Release 12.6 and later versions is SNMP Version 3 (SNMPv3) compliant. The following is the main SNMP MIB supported by Unified SRST:

- CISCO-SRST-MIB

For information on configuration of SNMP version 3 on Unified SRST router, see SNMP Configuration Guide.

Licensing

Cisco Unified SRST Permanent License

When you purchase a Cisco Unified SRST permanent license, the permanent license is installed on the device when the product is shipped to you. A permanent license never expires and you will gain access to that particular feature set for the lifetime of the device across all IOS release. If you purchase a permanent license for Cisco Unified SRST, you do not have to go through the Evaluation Right to Use and Right To Use (RTU) licensing processes for using the features. If you want to purchase a CME-SRST license for your existing device, you have to go through the RTU licensing process for using the features. There is no change in the existing process for purchasing the license.

The Cisco Unified SRST permanent license is available in the form of an XML cme-locked3 file. You must get the XML file and load it in the flash memory of the device. To install the permanent license from the command prompt, use the license install flash0:cme-locked3 command. The cme-locked3 is the XML file of the license.

Cisco Smart License

From Release 12.1 onwards, Unified SRST supports Smart Licensing, apart from the existing CSL licensing model. Smart Licensing is supported only on Cisco 4000 Series Integrated Services Router. Depending on the technology package available on the router, licenses such as UCK9 and Security are supported using Smart Licensing.

Smart Software Licensing is Cisco’s new licensing model that gives you visibility into license ownership and consumption. Smart licenses is managed by a cloud-based deployment model, namely Cisco Smart Software Manager (CSSM), or an on-prem software, Smart Software Manager satellite. Unified SRST supports both CSSM and satellite. Your access to the customer Smart Account residing on CSSM is authenticated using valid Cisco credentials. With the Smart Licensing support for Unified SRST, your device can register with CSSM or Cisco Smart Software Manager satellite. You can access your Licenses at the Cisco Software Central.
Unified SRST must register with CSSM or Cisco Smart Software Manager satellite to report license consumption. You can register Unified SRST to a Virtual Account within a Smart Account by generating a token ID from it, and pasting it to the underlying platform, Cisco 4000 Series Integrated Services Router. Once the token is generated, it can be used to register many other product instances in your network.

On the Unified SRST router, you need to ensure that the call home feature is not disabled. Also, Smart Licensing must be enabled at the router using the CLI command `license smart enable`. Use the `no` form of the command to disable Smart Licensing.

For more information on configuring Smart Licensing in your router, see Cisco 4000 Series ISRs Software Configuration Guide. For more information on configuring Call Home for your devices, see Configure Call Home, page 42. Once Smart Licensing is enabled, the router enters a 90-day evaluation period that persists until it registers to CSSM or the Cisco Smart Software Manager satellite.

You can register the router to CSSM or Cisco Smart Software Manager satellite with the token ID. To register the device (Unified SRST router) with CSSM or Cisco Smart Software Manager satellite, use the CLI command `license smart register idtoken`. For information on registering the device with CSSM, see Device Registration, Software Activation Configuration Guide, Cisco IOS Release 15M&T.

Upon successful registration, Unified SRST is in Registered status. As part of the registration process, the router sends an authorization request, indicating the number of phone endpoints defined by the `max-pool`, for SIP SRST, and `max-ephone`, for SCCP SRST. Based on the licenses in the Smart Account, CSSM or Cisco Smart Software Manager satellite responds with one of the defined statuses such as Authorized (using less than or equal to the number of licenses provisioned in CSSM or Cisco Smart Software Manager satellite) or Out-of-Compliance (using more than it has licenses for).

The license limit on Unified SRST is restricted by the maximum platform limit defined for the Unified SRST router (a cumulative sum of phones configured under `max-pool` and `max-ephone`). Hence, the license usage count cannot exceed the platform limit set for the Unified SRST router even when the cumulative sum of phones configured under `max-pool` and `max-ephone` exceeds the defined platform limit. For more details on the platform limit defined for Unified SRST, see Cisco Unified SRST/E-SRST 12.1 Supported Firmware, Platforms, Memory, and Voice Products.

CSSM or Smart Software Manager satellite reports license consumption submitted by the platform in its User Interface (UI), and subtracts it from the available licenses in the Virtual Account within the Smart Account. Unified SRST supports only one license entitlement to validate phones configured on Unified SRST.

SRST_EP —This license type supports all phones configured on Unified SRST.

---

**Note**

The SRST_EP license count reflects the total phone count of both the ephones and pools that are configured in the Unified SRST irrespective of whether the phones are registered or not.

Unified SRST sends an authorization request when a license consumption changes or every 30 days to let CSSM or Cisco Smart Software Manager satellite know it’s still available and communicating. The ID certificate issued to identify Unified SRST at time of registration is valid for one year, and is automatically renewed every six months.

---

**Note**

If the router does not communicate with CSSM or Cisco Smart Software Manager satellite for 90 days, the license authorization expires. When the license authorization expires, the devices registered on Unified SRST change status to Out of Compliance.
Chapter 2  Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Licensing

The license count is evaluated for the number of phones configured across the routers. The CSSM Licenses page reflects the total license count usage. The total number of licenses available for a type of license (Quantity), number of licenses currently used (In Use), and the number of unused or over-used licenses (Surplus or Shortage). If you do not have enough Cisco Smart licenses, you are in Out-of-Compliance state.

For example, consider a smart account in CSSM with 50 SRST_EP licenses. If you have a registered Unified SRST with 20 phones configured, the CSSM licenses page reflects Quantity as 50, In Use as 20, and Surplus as 30. For more information on Smart Software Manager, see Cisco Smart Software Manager User Guide.

For more information on switching between CSL and Cisco Smart License, see Licensing Modes, page 43.

The license entitlement for Unified SRST smart license is displayed on the router as follows:

```
Router# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ABC
  Virtual Account: XYZ
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jun 07 12:08:10 2017 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCESS
  Next Communication Attempt: Apr 13 07:11:48 2017 UTC

License Usage:
  License                  Entitlement tag            Count   Status
  --------------------------------------------------------------
  regid.2014-12.com.ci...  (ISR_4351_UnifiedCommun..)  1       AUTHORIZED
  regid.2016-10.com.ci...  (SRST_EP)                   4       AUTHORIZED
```

Configure Call Home

To configure the call home destination address and proxy server details for the HTTP proxy request, perform the following steps.

**Prerequisites**
- Cisco Smart Software Licensing is enabled.

**SUMMARY STEPS**

1. `configure terminal`
2. `call-home destination address http url`
3. `call-home http-proxy proxy_address port port number`
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><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>call-home destination address http url</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# call-home destination address http http://10.22.183.117:8080/ddce/services/DDCEService</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>call-home http-proxy proxy_address port port number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# call-home http-proxy 7.7.7.7 port 3218</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# end</code></td>
</tr>
</tbody>
</table>

Licensing Modes

From Unified SRST 12.1 onwards, both CSL and Smart Licensing modes are supported. That is, you can continue with CSL by not enabling Smart Licensing. Alternatively, they can enable Smart Licensing and decide later to go back to CSL by disabling Smart Licensing with the `no license smart enable` command. When you switch to CSL from the Smart Licensing mode, you must ensure that the End User License Agreement (EULA) is signed. CSL is not supported unless the EULA is signed. Use the CLI command `license accept end user agreement` in global configuration mode to configure EULA.

To verify the status of the license issued to phones registered on Unified SRST, you can use the `show license` command.

Router# `show license`?
  all      Show license all information
  status   Show license status information
  summary  Show license summary
  tech     Show license tech support information
  udi      Show license udi information
  usage    Show license usage information
Restrictions

- For the Unified SRST license, the UCK9 technology package must be available if the Collaboration Professional Suite package is not installed.

To purchase a license, go to http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key. To activate cme-srst feature license, see the Activating CME-SRST Feature License document.

Configure SIP Registrar Functionality for SIP Phones on Unified SRST

Session Initiation Protocol (SIP) registrar functionality in Cisco IOS software is an essential part of Cisco Unified SIP Survivable Remote Site Telephony (SRST). According to RFC 3261, a SIP registrar is a server that accepts Register requests.

Unified SIP SRST provides backup to Cisco Unified Communications Manager. The registrar functionality is configured on the Unified SRST gateway so as to assist fallback of endpoints to Unified SRST from Unified Communications Manager.

These services are used by a SIP IP phone if there is a WAN connection outage, and the SIP phone is unable to communicate with its primary SIP call control (IP-PBX). The Unified SIP SRST device also provides PSTN gateway access for placing and receiving PSTN calls.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. allow-connections sip to sip
5. sip
6. registrar server [expires [max sec] [min sec]]
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: Router&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: Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Configure SIP Registrar Functionality for SIP Phones on Unified SRST

### Command or Action | Purpose
--- | ---
**Step 3** | voice service voip
Example:
Router(config)# voice service voip
Enters voice service configuration mode.

**Step 4** | allow-connections sip to sip
Example:
Router(config-voi-srv)# allow-connections sip to sip
Allows connections from SIP to SIP endpoints.

**Step 5** | sip
Example:
Router(config-voi-srv)# sip
Enters SIP configuration mode.

**Step 6** | registrar server \[expires \[max sec \] \[min sec \]]\]
Example:
Router(conf-serv-sip)# registrar server expires max 600 min 60
Enables SIP registrar functionality. The keywords and arguments are defined as follows:

- **expires**: (Optional) Sets the active time for an incoming registration.
- **max sec**: (Optional) Maximum expiration time for a registration, in seconds. The range is from 600 to 86400. The default is 3600.
- **min sec**: (Optional) Minimum expiration time for a registration, in seconds. The range is from 60 to 3600. The default is 60.

**Note**
Ensure that the registration expiration timeout is set to a value smaller than the TCP connection aging timeout to avoid disconnection from the TCP.

**Step 7** | end
Example:
Router(conf-serv-sip)# end
Returns to privileged EXEC mode.

---

### Configure Back up Registrar Service to SIP Phones

Backup registrar service to SIP IP phones can be provided by configuring a voice register pool on SIP gateways. The voice register pool configuration provides registration permission control and can be used to configure some dial-peer attributes that are applied to the dynamically created VoIP dial peers when SIP phone registrations match the pool. The following call types are supported:

- SIP IP phone to or from:
  - Local PSTN
  - Local analog FXS phones
Configure SIP Registrar Functionality for SIP Phones on Unified SRST

- Local SIP IP phone

The commands in the configuration provide registration permission control and set up a basic voice register pool. The pool gives users control over which registrations are accepted by a Cisco Unified SIP SRST device and which can be rejected. Registrations that match this pool create VoIP SIP dial peers with the dial-peer attributes set to these configurations. Although only the `id` command is mandatory, this configuration example shows basic functionality.

**Prerequisites**

- The SIP registrar must be configured before a voice register pool is set up.

**Restrictions**

- The `id` command identifies the individual SIP IP phone or sets of SIP IP phones that are to be configured. Thus, the `id` command configured in Step 5 is required and must be configured before any other voice register pool commands. For Unified SRST, it is recommended to configure `id ip/network/device-id-name` and avoid using `id mac`.

**Note**

It is recommended that `id mac` command is not configured for Unified SRST, as the phones falling back from Unified Communications Manager to Unified SRST do not mostly fall back on the same network.

**Note**

The command `proxy` described in Step 7 is an optional configuration.

**Note**

To monitor SIP proxies, the `call fallback active` command must be configured, as described in Step 3.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `call fallback active`
4. `voice register pool tag`
5. `id [{network address mask | ip address mask | mac address }] [device-id-name devicename]`
6. `preference preference-order`
7. `proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]` (Optional)
8. `voice-class codec tag`
9. `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> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> call fallback active</td>
<td>(Optional) Enables a call request to fall back to alternate dial peers if there is network congestion.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config)# call fallback active</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice register pool tag</td>
<td>Enters voice register pool configuration mode for SIP phones.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config)# voice register pool 12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> id ([network address mask mask</td>
<td>ip address mask mask</td>
</tr>
<tr>
<td><em>Example:</em> Router(config-register-pool)# id network 172.16.0.0 mask 255.255.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> preference preference-order</td>
<td>Sets the preference order for the VoIP dial peers to be created. Range is from 0 to 10. Default is 0, which is the highest preference.</td>
</tr>
<tr>
<td><em>Example:</em> Router(config-register-pool)# preference 2</td>
<td></td>
</tr>
</tbody>
</table>
## Configure Backup Registrar Service to SIP Phones (Using Optional Commands)

The prior configurations set up a basic voice register pool. The configuration in this procedure adds optional attributes to increase functionality. As part of this configuration, you can support:

- **Translation Profile**—Applies the translation profile to a specific directory number or to all directory numbers on a SIP phone.
- **Alias**—Allows Cisco Unified SIP IP Phones to handle inbound PSTN calls to phone numbers that are unavailable when the main SIP call control (IP-PBX) is not available.
- **Class of restriction (COR)**—COR specifies which incoming dial peers can use which outgoing dial peers to make a call. Each dial peer can be provisioned with an incoming and outgoing COR list.

### Command or Action

| Step 7 | proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]] |
|--------|-------------------------------------------------------------------------------------------|

**Example:**

```console
Router(config-register-pool)# proxy 10.2.161.187 preference 1
```

(Optional) Autogenerates additional VoIP dial peers to reach the main SIP proxy whenever a Cisco Unified SIP IP Phone registers with a Cisco Unified SIP SRST gateway. The keywords and arguments are defined as follows:

- **ip-address**: IP address of the SIP proxy.
- **preference value**: (Optional) Defines the preference of the proxy dial peers that are created. The preference must be less (higher priority) than the preference configured with the `preference` command.
  
  Range is from 0 to 10. The highest preference is 0. There is no default.
- **monitor probe**: (Optional) Enables monitoring of proxy dial peers.
- **icmp-ping**: Enables monitoring of proxy dial peers using ICMP ping.
- **rtr**: Enables monitoring of proxy dial peers using RTR probes.
- **alternate-ip-address**: (Optional) Enables monitoring of alternate IP addresses other than the proxy address. For example, to monitor a gateway front end to a SIP proxy.

**Note**

The dial peer on which the probe is configured will be excluded from call routing only for outbound calls. Inbound calls can arrive through this dial peer.

### Command or Action

<table>
<thead>
<tr>
<th>Step 8</th>
<th>voice-class codec tag</th>
</tr>
</thead>
</table>

**Example:**

```console
Router(config-register-pool)# voice-class codec 15
```

Sets the voice class codec parameters. The `tag` argument is a codec group number between 1 and 10000.

### Command or Action

<table>
<thead>
<tr>
<th>Step 9</th>
<th>end</th>
</tr>
</thead>
</table>

**Example:**

```console
Router(config-register-pool)# end
```

Returns to privileged EXEC mode.
Prerequisites

- Before configuring the 'alias' command, translation rules must be set using the translation-profile outgoing (voice register pool) command.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool tag
4. translation-profile outgoing profile-tag
5. alias tag pattern to target [preference value]
6. cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [- ending-number] | default}
7. incoming called-number [number]
8. number tag number-pattern [preference value] [huntstop]
9. dtmf-relay [cisco-rtp] [rtp-nte] [sip-notify]
10. 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></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register pool tag</td>
<td>Enters voice register pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td>Router(config)# voice register pool 12</td>
<td></td>
</tr>
</tbody>
</table>
### Configure SIP Registrar Functionality for SIP Phones on Unified SRST

#### Chapter 2  Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

#### Step 4

**translation-profile outgoing profile-tag**

**Example:**
```
Router(config-register-pool)#
voice translation-rule 1
  rule 1 /1000/ /1006/
!
voice translation-profile 1
  translate called 1
!
voice register pool xxx
  translation-profile outgoing 1
```

Use this command to apply the translation profile to a specific directory number or to all directory numbers on a SIP phone.

- **Profile-tag:** Translation profile name to handle translation to outgoing calls.

#### Step 5

**alias tag pattern to target [preference value]**

**Example:**
```
Router(config-register-pool)# alias 1 94... to 91011 preference 8
```

Allows Cisco Unified SIP IP Phones to handle inbound PSTN calls to phone numbers that are unavailable when the main proxy is not available. The keywords and arguments are defined as follows:

- **tag:** Number from 1 to 5 and the distinguishing factor when there are multiple alias commands.
- **pattern:** The prefix number; matches the incoming phone number and may include wildcards.
- **to:** Connects the tag number pattern to the alternate number.
- **target:** The target number; an alternate phone number to route incoming calls to match the number pattern.
- **preference value:** (Optional) Assigns a dial-peer preference value to the alias. The value argument is the value of the associated dial peer, and the range is from 1 to 10. There is no default.
## Configure SIP Registrar Functionality for SIP Phones on Unified SRST

### Chapter 2  Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

#### Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [-ending-number] | default}` | Configures a class of restriction (COR) on the VoIP dial peers associated with directory numbers. COR specifies which incoming dial peers can use which outgoing dial peers to make a call. Each dial peer can be provisioned with an incoming and outgoing COR list. The keywords and arguments are defined as follows:  
  - **incoming**: COR list to be used by incoming dial peers.  
  - **outgoing**: COR list to be used by outgoing dial peers.  
  - **cor-list-name**: COR list name.  
  - **cor-list-number**: COR list identifier. The maximum number of COR lists that can be created is four, comprised of incoming or outgoing dial peers.  
  - **starting-number**: Start of a directory number range, if an ending number is included. Can also be a standalone number.  
  - (Optional) Indicator that a full range is configured.  
  - **ending-number**: (Optional) End of a directory number range.  
  - **default**: Instructs the router to use an existing default COR list. |

**Example:**
```
Router(config-register-pool)# cor incoming call91 1 91011
```

#### Step 7

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>incoming called-number [number]</code></td>
<td>Applies incoming called parameters to dynamically created dial peers. The number argument is optional and indicates a sequence of digits that represent a phone number prefix.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-register-pool)# incoming called-number 308
```

#### Step 8

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `number tag number-pattern (preference value) [huntstop]` | Indicates the E.164 phone numbers that the registrar permits to handle the Register message from the Cisco Unified SIP IP Phone. The keywords and arguments are defined as follows:  
  - **tag**: Number from 1 to 10 and the distinguishing factor when there are multiple `number` commands.  
  - **number-pattern**: Phone numbers (including wildcards and patterns) that are permitted by the registrar to handle the Register message from the SIP IP phone.  
  - **preference value**: (Optional) Defines the number list preference order.  
  - **huntstop**: (Optional) Stops hunting if the dial peer is busy. |

**Example:**
```
Router(config-register-pool)# number 1 50.. preference 2
```
Chapter 2    Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Configure SIP Registrar Functionality for SIP Phones on Unified SRST

Verify SIP Registrar Configuration

To help you troubleshoot a SIP registrar and voice register pool, perform the following steps.

SUMMARY STEPS

1.  debug voice register errors
2.  debug voice register events
3.  show sip-ua status registrar

### Command or Action

**Step 9**

`dtmf-relay [cisco-rtp] [rtp-nte] [sip-notify]

Example:
Router(config-register-pool)# dtmf-relay rtp-nte

**Step 10**

`end`

Example:
Router(config-register-pool)# end

**Purpose**

Specifies how a SIP gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network. The keywords are defined as follows:

- **cisco-rtp**: (Optional) Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with a Cisco proprietary payload type.
- **rtp-nte**: (Optional) Forwards DTMF tones by using RTP with the Named Telephone Event (NTE) payload type.
- **sip-notify**: (Optional) Forwards DTMF tones using SIP NOTIFY messages.

Returns to privileged EXEC mode.
### 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>debug voice register errors</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Use this command to debug errors that happen during registration.</td>
</tr>
<tr>
<td>Router# debug voice register errors</td>
<td>If there are no voice register pools configured for a particular registration request, the message “Contact doesn’t match any pools” is displayed.</td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.523 PDT: VOICE_REG_POOL: Contact doesn't match any pools</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Register request for (33015) from (10.2.152.39)</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Contact doesn't match any pools.</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:55.559 PDT: VOICE_REG_POOL: Register request for (33017) from (10.2.152.39)</em></td>
<td></td>
</tr>
<tr>
<td>*Apr 22 11:53:04.559 PDT: VOICE_REG_POOL: Maximum registration threshold for pool(3) hit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>debug voice register events</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Using the <strong>debug voice register events</strong> command should suffice to display registration activity.</td>
</tr>
<tr>
<td>Router# debug voice register events</td>
<td>Registration activity includes matching of pools, registration creation, and automatic creation of dial peers. For more details and error conditions, you can use the <strong>debug voice register errors</strong> command.</td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Contact matches pool 1</td>
<td>The phone number 91011 registered successfully, and <strong>type 1</strong> is reported, which means there is a pre-existing VoIP dial peer.</td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) contact(192.168.0.2) add to contact table</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) exists in contact table</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: contact(192.168.0.2) exists in contact table, ref updated</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Created dial-peer entry of type 1</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Registration successful for 91011, registration id is 257</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>show sip-ua status registrar</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Use this command to display all the SIP endpoints currently registered with the contact address.</td>
</tr>
<tr>
<td>Router# show sip-ua status registrar</td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td>destination</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>91021</td>
<td>192.168.0.3</td>
</tr>
<tr>
<td>91011</td>
<td>192.168.0.2</td>
</tr>
<tr>
<td>95021</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95012</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95011</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95500</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>94011</td>
<td>10.2.161.40</td>
</tr>
<tr>
<td>94500</td>
<td>10.2.161.40</td>
</tr>
</tbody>
</table>
Verify Proxy Dial-Peer Configuration

To use the `icmp-ping` keyword with the `proxy` command to assist in troubleshooting proxy dial peers, perform the following steps.

**SUMMARY STEPS**

1. `configure terminal`
2. `voice register pool tag`
3. `proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]`
4. `end`
5. `show voice register dial-peers`
6. `show dial-peer voice`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Use this command to enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> voice register pool tag</td>
<td>Use this command to enter voice register pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice register pool 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> proxy ip-address [preference value] [monitor probe {icmp-ping</td>
<td>rtr}] [alternate-ip-address]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# proxy 10.2.161.187 preference 1 monitor probe icmp-ping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show voice register dial-peers</td>
<td>Use this command to verify dial-peer configurations, and notice that icmp-ping monitoring is set.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show voice register dial-peers dial-peer voice 40035 voip preference 5 destination-pattern 91011 session target ipv4:192.168.0.2 session protocol sipv2 voice-class codec 1 dial-peer voice 40036 voip preference 1 destination-pattern 91011 session target ipv4:10.2.161.187 session protocol sipv2 voice-class codec 1 monitor probe icmp-ping 10.2.161.187</td>
<td></td>
</tr>
</tbody>
</table>
Configure SIP Registrar Functionality for SIP Phones on Unified SRST

Step 6

Use the `show dial-peer voice` command on dial peer 40036, and notice the monitor probe status.

Example:
```
Router# show dial-peer voice
VoiceOverIpPeer40036
peer type = voice, information type = voice,
description = '',
tag = 40036, destination-pattern = '91011',
answer-address = '', preference=1,
CLID Restriction = None
CLID Network Number = ''
CLID Second Number sent
source carrier-id = '', target carrier-id = '',
source trunk-group-label = '', target
trunk-group-label = '',
numbering Type = 'unknown'
group = 40036, Admin state is up, Operation state is up,
incoming called-number = '', connections/maximum = 0/unlimited

! Default output for incoming called-number command
DTMF Relay = disabled,
modem transport = system,
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dns-map =
permission :both
incoming COR list :maximum capability

! Default output for cor command
outgoing COR list :minimum requirement

! Default output for cor command
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = '',
disconnect-cause = 'no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4
oldAddrFamily 4
type = volp, session-target = 'ipv4:10.2.161.187',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41, ip video rsvp-pass
DSCP = af41
ip video rsvp-fail DSCP = af41,
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-gos = best-effort, acc-gos = best-effort,
req-gos video = best-effort, acc-gos video = best-effort,
req-gos audio def bandwidth = 64, req-gos audio max
bandwidth = 0,
req-gos video def bandwidth = 384, req-gos video max
bandwidth = 0,
```

Note: Also highlighted is the output of the `cor` and `incoming called-number` commands.
Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy

From Unified SRST 12.6 Release (Cisco IOS XE Gibraltar 16.11.1a) onwards, all configurations on Unified SRST, Unified E-SRST, and Unified Secure SRST must meet the password policy.

**General Password Policy Guidelines:**

- Passwords must have a minimum of 6 alphanumeric characters, and a maximum of 15 alphanumeric characters.
- Passwords must not contain symbols or special characters.
- Passwords must contain at least one numeral, one uppercase alphabet, and one lowercase alphabet.

If the password is not configured as per the policy, the Unified SRST router displays an error message:

`Error: The password you have entered is incorrect. Your password must contain:`
Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy

1. A minimum of 6 and a maximum of 15 alphanumeric characters, excluding symbols and special characters.
2. A minimum of one numeral, one uppercase alphabet, and one lowercase alphabet.

The Unified CME password policy is applicable for Unified SRST configurations on Cisco IOS XE 16.11.1a and later. Unified SRST password policy is not applicable in the following scenarios:

- Upgrade from an older IOS version to Cisco IOS XE 16.11.1a
- Downgrade from Cisco IOS XE 16.11.1a to an older version

Guidelines for Password Configuration and Encryption

Configure the passwords relevant to Unified SRST, Unified E-SRST, and Unified Secure SRST using the CLI commands as follows:

- call-manager-fallback configuration mode
  - xml user username password [0|6] password privilege-level

Note: The 0 in the parameter [0|6] mentioned in the CLI command represents plain, unencrypted text and 6 represents level 6 password encryption.

- Apart from the parameter configurations ([0|6]) at the command level, configure the Unified SRST router to support encryption.
- Configure the CLI command encrypt password under call-manager-fallback configuration mode to support type 6 encryption on the Unified SRST router.
- Also, it is mandatory to configure key config-key password-encrypt [Master key] and password encryption aes to support encryption on the Unified SRST router.
- If the key used to encrypt the password is replaced with a new key (replace key or re-key), then the password is re-encrypted with the new key.
- You must adhere to SRST Password Policy for both type 0 and type 6 parameters that you configure on Unified SRST.
- Configure no encrypt password for type 0 password on the Unified SRST router. A type 0 password is displayed as unencrypted plain text.
- If you are performing a downgrade from Unified SRST 12.6 to an earlier version, then you must execute the CLI command no encrypt password. If the CLI command no encrypt password is configured, the password is presented as plain text.

Example

The following is a sample configuration on Unified SRST router to support password encryption:

```
Router(config)#key config-key password-encrypt <cisco123>
Router(config)#password encryption aes
Router(config)#call-manager-fallback
Router(config-cm-fallback)encrypt password
```

Deprecation of CLI commands

From Unified SRST Release 12.6 onwards, the following CLI commands that are configured under call-manager-fallback configuration mode are deprecated to enhance product security:
Chapter 2  Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy

- `log password password-string`
- `xmltest`
- `xmlschema schema-url`
- `xmlthread number`

### Removal of Passwords and Keys from Logs

From Unified SRST Release 12.6 onwards, passwords and sRTP keys are not printed to logs to enhance security of Unified SRST. The information about keys is available only in the show commands from Unified SRST 12.6 release onwards. The CLI command `show ephone offhook` for SCCP and `show sip-ua calls` for SIP are enhanced to display the keys that are in use per media stream, along with the sRTP Ciphers.

The following is a sample output for the show command, `show sip-ua calls`. The lines that are added to the show command output as part of the Unified SRST 12.6 enhancement are the local crypto key and the remote crypto key:

```
SIP UAC CALL INFO
Number of SIP User Agent Client(UAC) calls: 0
SIP UAS CALL INFO
Call 1
SIP Call ID : 007278df-12e00376-6ed02377-6ffbaca908.55.0.195
State of the call : STATE_ACTIVE (?)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 1001
Called Number : 6901%23
Called URI : sip:6901%23@8.39.25.11;user=phone
Bit Flags : 0x10C0401C 0x10000100 0x4
CC Call ID : 196
Local UUID : 61488a9100105000a000007278df12e0
Remote UUID : c4b7f9475629538096ef61699b96746f
Source IP Address (Sig ) : 8.39.25.11
Destn SIP Req Addr:Port : [8.55.0.195]:52704
Destn SIP Resp Addr:Port: [8.55.0.195]:52704
Destination Name : 8.55.0.195
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 : 196
Stream Type : voice+dtmf (1)
Stream Media Addr Type : 1
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [8.39.25.11]:8080
Media Dest IP Addr:Port : [8.55.0.195]:23022
Local Crypto Suite : AEAD_AES_256_GCM
Remote Crypto Suite : AEAD_AES_256_GCM (AEAD_AES_128_GCM
AEAD_AES_256_GCM
AEAD_AES_128_GCM
```
Chapter 2      Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Toll Fraud Prevention for SIP Line Side on Unified SRST

The following is a sample output for the show command, `show ephone offhook`. The lines that are added to the show command output as part of the Unified SRST 12.6 enhancement are local key and remote key.

ephone-1[0] Mac:549A.EBB5.8000 TCP socket:[1] activeLine:1 whisperLine:0 REGISTERED in SCCP

`ver 21/17 max_streams=1 + Authentication + Encryption with TLS connection`  
`mediaActive:1 whisper_mediaActive:0 startMedia:1 offhook:1 ringing:0 reset:0 reset_sent:0`  
`pacing:0 debug:0 caps:8 IP:8.44.22.63 * 17872 SCCP Gateway (AN) keepalive 28 max_line 1 available_line 1`  
`port 0/0/0 button 1: cw:1 ccw:(0 0) dn 1 number 6901 CM Fallback CH1 CONNECTED CH2 IDLE`  
`Preferred Codec: g711ulaw Lpcor Type: none Active Secure Call on DN 1 chan 1 :6901 8.44.22.63 18116`  
`to 8.39.25.11 8066 via 8.39.0.1 G711ulaw64k 160 bytes no vad`  
`SRTP cipher: AES_CM_128_HMAC_SHA1_32 local key: 0OPV0yxvcnRLPMzHfmYbwgHfdxcuS1uPbp5j/Tjk remote key: e8DQl3Kvk7LjZlipaCoMg9TMreBmiPsPmNlVhWIA`  
`Tx Pkts 0 bytes 0 Rx Pkts 0 bytes 0 Lost 0 Jitter 0 Latency 0 callingDn -1 calledDn -1`  

Toll Fraud Prevention for SIP Line Side on Unified SRST

Unified SRST Release 12.6 enhances the existing Toll Fraud Prevention feature by enforcing security on the SIP line side of Unified SRST. The feature enhancement secures the Unified SRST system against potential toll fraud exploitation by unauthorized users from the SIP line side.

![Note](image)

```
Unified SRST 8.1 to 12.5 Releases restricts toll fraud prevention only to securing calls over the SIP trunk. For more information about Toll Fraud Prevention over a SIP trunk, see Configuring a Trusted IP Address List for Toll-Fraud Prevention.
```

Some of the key features of Toll Fraud Prevention on Unified SRST for secure calls over SIP lines are:

- Authenticates all the SIP line messages that are triggered from the endpoints to Unified SRST.
- If the IP address of the endpoint is not part of the IP address trusted list, the call is rejected by Unified SRST.
- Unified SRST authenticates both IPv4 an IPv6 addresses as part of the toll fraud prevention mechanism.

**Prerequisites for Configuring Toll Fraud Prevention for SIP Line Side**

- Unified SRST 12.6 or a later version.
- Cisco IOS XE Gibraltar Release 16.11.1a or later.
Configuration Recommendations for Toll Fraud Prevention on Unified SRST

Unified SRST 12.6 enforces security and toll fraud prevention for SIP line side on Unified SRST. The `ip address trusted authentication` configuration blocks unauthorized calls from the line side. Hence, the toll fraud prevention feature secures Unified SRST 12.6 and later from unauthorized users on the line side.

The IP addresses of SRST endpoints are available before registration with Unified SRST, as they are configured (under `voice register pool`) for fallback from Unified CM. Hence, it is not mandatory that the endpoints are registered to Unified SRST for configuring toll fraud prevention.

The IP trust list for Unified SRST is populated based on the IP address information available under `voice register pool` configuration mode. You can find the IP address of the SIP endpoints on Unified SRST under the following commands in voice register pool configuration mode:

- `id ip` (For example, `id ip 192.168.0.0`)
- `id network` (For example, `id network 192.168.25.0 mask 255.255.255.0`)

Sometimes, IP addresses of endpoints are not available to Unified SRST before registration. Consider a scenario where `id device-id` is the CLI command configured under voice register pool configuration mode to define the device name. Then, the IP address of the device or endpoint is available to Unified SRST only during registration.

The following are the configurations of Toll Fraud Prevention in Unified SRST, 12.6:

- The CLI command `ip address trusted authentication` is enabled by default in Unified SRST. The command `ip address trusted authentication` ensures that security is enabled on the Unified SRST system.
- You can manually configure your Unified SRST endpoints as trusted by entering the IP address or subnet of the trusted phone under the `iptrust-list` configuration mode, as follows:

```
Router#config t
Router(config)#voice service voip
Router(conf-voi-serv)#ip address trusted list
Router(cfg-iptrust-list)#ipv4 192.168.10.0 /16
OR
Router(cfg-iptrust-list)#ipv4 192.168.12.0 255.255.255.0
```

- You can verify the manually added IP address of the Unified SRST endpoint, as follows:

```
Router#show running-config | section voice service voip
voice service voip
  ip address trusted list
  ipv4 192.168.10.0 /16
  ipv4 192.168.12.0 255.255.255.0
```

- The CLI command `ip address trusted list` under `voice service voip` configuration mode supports manual configuration of trusted IP addresses.
- The CLI command `show ip address trusted check` provides information on whether a particular IP address is trusted or not.
- The CLI command `silent-discard untrusted` in `sip` configuration mode silently discards SIP requests from untrusted sources. This command is enabled by default on Unified SRST.
- The `show ip address trusted list` CLI command displays a list of trusted IP addresses. The trusted IP addresses are displayed under the following lists:
- Dial Peer (only applicable for trunk side): Provides details on the IP address of the trunk that is configured under the dial-peer configuration mode.
- Configured IP Address Trusted List: Provides details on the manually configured IP addresses that are trusted.
- Dynamic IP Address Trusted List: Provides details on the IP address of all the phones that are configured for fallback from Unified CM. This list is introduced in Unified CME 12.6 Release.
- Server Group: Provides details on the IP address of the phones that are configured under server-groups configuration mode.

Router>enable
Router#show ip address trusted list
IP Address Trusted Authentication
  Administration State: UP
  Operation State: UP

IP Address Trusted Call Block Cause: call-reject (21)

VoIP Dial-peer IPv4 and IPv6 Session Targets:
Peer Tag Oper State Session Target
-------- ---------- --------------
4          UP         ipv4:10.65.125.155

Configured IP Address Trusted List:
ipv4 192.168.20.1
ipv4 192.168.20.2 255.255.0.0
ipv4 192.168.20.3 255.255.0.0
ipv4 192.168.20.4 255.255.255.0

Dynamic IP Address Trusted List:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Count</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4:8.55.0.0</td>
<td>255.255.0.0</td>
<td>1</td>
<td>Pool Configured</td>
</tr>
<tr>
<td>ipv4:192.168.0.1</td>
<td>255.255.0.0</td>
<td>2</td>
<td>Pool Configured</td>
</tr>
<tr>
<td>ipv6:2001:420:54FF:13::312:0</td>
<td>119</td>
<td>1</td>
<td>Phone Registered</td>
</tr>
</tbody>
</table>

Note: The column Count in Dynamic IP Address Trusted List displays the number of directory numbers (DNs) sharing the same IP address. For example, ipv4 192.168.0.1 with count 2 represents two DNs sharing the IP address 192.168.0.1.

Note: The output of show ip address trusted list command displays the entry in column Type as ‘Phone Registered’ if id device-id is configured.

Upgrade Considerations

When you upgrade to Unified SRST 12.6 version, you need not perform extra configurations for supporting toll fraud prevention. All the endpoints that are manually configured or auto-registered on Unified SRST are added to the Unified SRST IP Address Trust List. You can view the list of trusted IP addresses under the output of the CLI command show ip address trusted list.
Configure Toll Fraud Prevention

This section contains the following tasks.

- Configure IP Address Trusted Authentication for Incoming VoIP Calls, page 63
- Add Valid IP Addresses For Incoming VoIP Calls, page 65
- Troubleshooting Tips for Toll Fraud Prevention, page 67

Configure IP Address Trusted Authentication for Incoming VoIP Calls

Prerequisites

- Unified SRST 8.1 or a later version for secure trunk calls.
- Unified SRST 12.6 or a later version for secure line and trunk calls.
- The CLI command `silent-discard untrusted` needs to be configured for the feature to work

Restrictions

- For an incoming VoIP call, IP trusted authentication must be invoked when the IP address trusted authentication is in “UP” operational state.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. ip address trusted authenticate
5. ip-address trusted call-block cause `<code>`
6. end
7. show ip address trusted list
## Configure Toll Fraud Prevention

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service voip configuration mode.</td>
<td>Router(config)# voice service voip</td>
</tr>
<tr>
<td>Step 4 ip address trusted authenticate</td>
<td>Enables IP address authentication on incoming H.323 or SIP trunk calls for toll fraud prevention support.</td>
<td>Router(conf-voi-serv)# ip address trusted authenticate</td>
</tr>
<tr>
<td>Step 5 ip-address trusted call-block cause code</td>
<td>Issues a cause-code when the incoming call is rejected to the IP address trusted authentication. This command is enabled by default.</td>
<td>Router(conf-voi-serv)#ip address trusted call-block cause call-reject</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Returns to privileged EXEC mode.</td>
<td>Router(#) end</td>
</tr>
<tr>
<td>Step 7 show ip address trusted list</td>
<td>Verifies a list of valid IP addresses.</td>
<td>Router# #show ip address trusted list</td>
</tr>
</tbody>
</table>

**Note**

If the IP address trusted authentication fails, a call-reject (21) cause-code is issued to disconnect the incoming VoIP call.

### Examples

- Router>enable
Chapter 2 Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Configure Toll Fraud Prevention

Router#show ip address trusted list
IP Address Trusted Authentication
Administration State: UP
Operation State: UP

IP Address Trusted Call Block Cause: call-reject (21)

VoIP Dial-peer IPv4 and IPv6 Session Targets:
Peer Tag Oper State Session Target
-------- ---------- --------------
Configured IP Address Trusted List:
ipv4 192.168.20.1
ipv4 192.168.20.2 255.255.0.0
ipv4 192.168.20.3 255.255.0.0
ipv4 192.168.20.4 255.255.255.0

Dynamic IP Address Trusted List:
IP Address Subnet Mask Count Type
---------------------------------- --------------- ----- ----------------
ipv4:8.55.0.0 255.255.0.0 1 Pool Configured
ipv4:192.168.0.1 255.255.0.0 1 Pool Configured

Add Valid IP Addresses For Incoming VoIP Calls

Prerequisites

- Cisco Unified CME 8.1 or a later version.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. ip address trusted list
5. ipv4 ipv4 address network mask
6. end
7. show ip address trusted list
Chapter 2      Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

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>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service voip configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 ip address trusted list</td>
<td>Enters ip address trusted list mode and allows to manually add additional valid IP addresses.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# ip address trusted list</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-iptrust-list)#</td>
<td></td>
</tr>
<tr>
<td>Step 5 ipv4 {&lt;ipv4 address&gt; [&lt;network mask&gt;]}</td>
<td>Allows you to add up to 100 IPv4 addresses in ip address trusted list. Duplicate IP addresses are not allowed in the ip address trusted list.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-iptrust-list)#ipv4 172.19.245.1</td>
<td></td>
</tr>
<tr>
<td>Router(conf-iptrust-list)#ipv4 172.19.243.1</td>
<td></td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-register-pool)# end</td>
<td></td>
</tr>
<tr>
<td>Step 7 show ip address trusted list</td>
<td>Displays a list of valid IP addresses for incoming H.323 or SIP trunk calls.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show shared-line</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example shows three IP addresses configured as trusted IP addresses:

```
Router# show ip address trusted list
IP Address Trusted Authentication
   Administration State: UP
   Operation State:     UP

   IP Address Trusted Call Block Cause: call-reject (21)

   Configured IP Address Trusted List:
      ipv4 192.168.20.1
      ipv4 192.168.20.2 255.255.0.0
      ipv4 192.168.20.3 255.255.0.0
      ipv4 192.168.20.4 255.255.255.0
```
Troubleshooting Tips for Toll Fraud Prevention

For troubleshooting toll fraud mechanism supported on Unified SRST, you can enable the CLI commands `debug voip iptrust debug` and `debug voip iptrust detail`, as follows:

```
Router#debug voip iptrust
voip iptrust debugging is on
Router#debug voip iptrust detail
voip iptrust detail debugging is on
```

IPv6 Support for Unified SRST SIP IP Phones

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP). IPv6 uses packets to exchange data, voice, and video traffic over digital networks. Also, IPv6 increases the number of network address bits from 32 bits in IPv4 to 128 bits. From Unified SRST Release 12.0 onwards, Unified SRST supports IPv6 protocols for SIP IP phones.

IPv6 support in Unified SRST allows the network to behave transparently in a dual-stack (IPv4 and IPv6) environment and provides additional IP address space to SIP IP phones that are connected to the network. If you do not have a dual-stack configuration, configure the CLI command `call service stop` under `voice service voip` configuration mode before changing to dual-stack mode. For an example of switching to dual-stack mode, see Examples for Configuring IPv6 Pools for SIP IP Phones, page 92.

The Cisco IP Phone 7800 Series and 8800 Series are supported on IPv6 for Unified SRST.

For more information on configuring SIP IP phones for IPv6 source address, see Configure IPv6 Pools for SIP IP Phones, page 68.

For an example of configuring IPv6 Support on Unified SRST, see Examples for Configuring IPv6 Pools for SIP IP Phones, page 92.


Feature Support for IPv6 in Unified SRST SIP IP Phones

The following basic features are supported for a IPv6 WAN down scenario:

- Basic SIP Line (IPv4 or IPv6) to SIP Line calls (IPv4 or IPv6) when Unified SRST is in dual-stack `no anat` mode.

The following supplementary services are supported as part of IPv6 in Unified SRST IP Phones:

- Hold/Resume
- Call Forward
- Call Transfer
- Three-way Conference (with BIB conferencing only)
- Line to T1/E1 Trunk and Trunk to Line with Supplementary Service Features
- Fax to and from PSTN (IPv4 ATA to ISDN T1/E1) for both T.38 Fax Relay and Fax Passthrough

Restrictions

The following are the known restrictions for IPv6 support on Unified SRST:
IPv6 Support for Unified SRST SIP IP Phones

- SIP Trunks are not supported on Unified SRST for IPv6 deployment. PSTN calls are supported only through T1/E1 trunks.
- SCCP IP Phones are not supported in a deployment of IPv6 for Unified SRST.
- SIP Phones can be either in IPv4 only or IPv6 only mode (no anat).
- Trancoding and Transrating are not supported.
- H.323 trunks are not supported.
- Secure SIP lines or trunks are not supported.
- IPv6 on Unified SRST is not supported on the Cisco IOS platform. The support is restricted to Cisco IOS XE platform with Cisco IOS Release 16.6.1 or later versions.

Configure IPv6 Pools for SIP IP Phones

Before You Begin
- Unified SRST 12.0 or a later version.
- IPv6 option only appears if protocol mode is dual-stack configured under sip-ua configuration mode or IPv6.
- Cisco Unified SRST License must be configured for the gateway to function as a Unified SRST gateway to support IPv6 functionality. For more information on licenses, see Licensing, page 40.
- Cisco Unified Communications Manager (Unified Communications Manager) is provisioned with the IPv6 address of Unified SRST. For information on configuration of Unified SRST on Unified Communications Manager, see the section Survivable Remote Site Telephony Configuration in Cisco Unified Communications Manager Administration Guide.

SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 unicast-routing
4. voice service voip
5. sip
6. no anat
7. call service stop
8. exit
9. exit
10. sip-ua
11. protocol mode {ipv4 | ipv6 | dual-stack [preference {ipv4 | ipv6}]}
12. exit
13. voice service {voip}
14. sip
15. no call service stop
16. exit
17. voice register global
18. default mode
19. max-dn max-directory-numbers
20. max-pool max-voice-register-pools
21. exit
22. voice register pool pool-tag
23. id { network address mask | ip address mask | mac address }
24. end
### IPv6 Support for Unified SRST SIP IP Phones

#### 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>Router&gt; enable</td>
<td></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>Router #configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 unicast-routing</td>
<td>Enables the forwarding of IPv6 unicast datagrams.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice service voip</td>
<td>Enters voice-service configuration mode to specify a voice encapsulation type.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td>Specifies Voice over IP (VoIP) parameters.</td>
</tr>
<tr>
<td><strong>Step 5</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> no anat</td>
<td>Disables Alternative Network Address Types (ANAT) on a SIP trunk.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-serv-sip)# no anat</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> call service stop</td>
<td>Shuts down SIP call service.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-serv-sip)# call service stop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### IPv6 Support for Unified SRST SIP IP Phones

**Step 9**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits voice service voip configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-voi-serv)# exit
```

**Step 10**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sip-ua</code></td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config)# sip-ua
```

**Step 11**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`protocol mode {ipv4</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-sip-ua)# protocol mode dual-stack preference ipv6
```

- ipv4—Allows you to set the protocol mode as an IPv4 address.
- ipv6—Allows you to set the protocol mode as an IPv6 address.
- dual-stack—Allows you to set the protocol mode for both IPv4 and IPv6 addresses.
- preference—Allows you to choose a preferred IP address family if protocol mode is dual-stack.

**Step 12**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits SIP configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-sip-ua)# exit
```

**Step 13**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>voice service {voip}</code></td>
<td>Enters voice-service configuration mode to specify a voice encapsulation type.</td>
</tr>
</tbody>
</table>

**Example:**

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

- voip—Specifies Voice over IP (VoIP) parameters.

**Step 14**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sip</code></td>
<td>Enters SIP configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-voi-serv)# sip
```
## IPv6 Support for Unified SRST SIP IP Phones

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td><code>no call service stop</code></td>
<td>Activates SIP call service.</td>
</tr>
</tbody>
</table>
|      | **Example:**  
|      | `Router(config-serv-sip)# call service stop` |           |
| 16   | `exit` | Exits SIP configuration mode. |
|      | **Example:**  
|      | `Router(config-serv-sip)# exit` |           |
| 17   | `voice register global` | Enters voice register global configuration mode to set parameters for all supported SIP phones in Unified SRST. |
|      | **Example:**  
|      | `Router(config)# voice register global` |           |
| 18   | `default mode` | Enables mode for provisioning SIP phones in Unified SRST. The default mode is Unified SRST itself. |
|      | **Example:**  
|      | `Router(config-register-global)# default mode` |           |
| 19   | `max-dn max-directory-numbers` | Limits number of directory numbers to be supported by this router.  
|      | **Example:**  
|      | `Router(config-register-global)# max-dn 50` | Maximum number is platform and version-specific.  
|      |   | Type ? for value. |
| 20   | `max-pool max-voice-register-pools` | Sets maximum number of SIP phones to be supported by the Unified SRST router. |
|      | **Example:**  
|      | `Router(config-register-global)# max-pool 40` |           |
| 21   | `exit` | Exits voice register global configuration mode. |
|      | **Example:**  
|      | `Router(config-register-global)# exit` |           |
| 22   | `voice register pool pool-tag` | Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone. |
|      | **Example:**  
|      | `Router(config)# voice register pool 1` |           |
Configure Unified SRST on Cisco 4000 Series Integrated Services Platform

For Unified SRST Release 10.5 and later, Unified SRST is supported on Cisco 4000 Series Integrated Services Routers. A Unified SRST system supports SIP phones with standard-based RFC 3261 feature support locally and across SIP WAN networks. With Cisco Unified SIP SRST, SIP phones can place calls across SIP networks with similar features, as SCCP phones do. For example, most SCCP phone features such as caller ID, speed dial, and redial are supported on SIP networks, that give users the opportunity to choose SCCP or SIP.

Prerequisites

- Cisco IOS XE Denali 16.3.1 or a later release.
- Cisco IP Phones 7800 Series or 8800 Series.
- An appropriate feature license to support Unified SIP SRST on the router.
- You need to configure voice register global in your router.
- You need to ensure that your router is in default mode (for Unified SRST).

Restrictions

- For a list of restrictions for Unified SIP SRST support on Cisco 4000 Series Integrated Services Routers, see Restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers, page 37.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip

Command or Action | Purpose
--- | ---
Step 23 | id \{ network address mask | ip address mask | mac address \}
| | Explicitly identifies a locally available individual SIP phone to support a degree of authentication.

Example:
Router(config-register-pool)# id network 2001:420:54FF:13::901:0/117
Router(config-register-pool)# id network 10.64.88.0 mask 255.255.255.0

Step 24 | end
| | Exits to privileged EXEC mode.

Example:
Router(config)# end
4. allow-connections from-type to to-type
5. no supplementary-service sip moved-temporarily
6. no supplementary-service sip refer
7. supplementary-service media-renegotiate
8. sip
9. registrar server [expires[max sec][min sec]]
10. exit
11. exit
12. voice register global
13. default mode
14. max-dn max-directory-numbers
15. max-pool max-voice-register-pools
16. exit
17. voice register pool pool-tag
18. id [network address mask | ip address mask]
19. dtmf-relay [rtp-nte]
20. codec codec
21. no vad
22. 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>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice-service configuration mode and specifies voice-over-IP encapsulation.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters voice register global configuration mode to set global parameters for all supported Cisco SIP IP phones in a Cisco Unified SIP SRST environment.</td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 allow-connections from-type to to-type</td>
<td>Allows connections between specific types of endpoints in a VoIP network.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# allow-connections sip to sip</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> no supplementary-service sip moved-temporarily</td>
<td>Disables supplementary service for call forwarding.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# no supplementary-service sip moved-temporarily</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> no supplementary-service sip moved-temporarily</td>
<td>Prevents the router from forwarding a REFER message to the destination for call transfers.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# no supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> supplementary-service media-renegotiate</td>
<td>Enables mid-call media renegotiation for supplementary services.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# supplementary-service media-renegotiate</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# sip</td>
<td>• Required only if you perform the following step for enabling the SIP registrar function.</td>
</tr>
<tr>
<td><strong>Step 9</strong> registrar server [expires[max sec]min sec]]</td>
<td>Enables SIP registrar functionality in Unified SRST.</td>
</tr>
<tr>
<td>Example: Router(config-serv-sip)# registrar server expires max 120 min 60</td>
<td>• expires: (Optional) Sets the active time for an incoming registration.</td>
</tr>
<tr>
<td></td>
<td>• max sec—(Optional) Maximum time for a registration to expire, in seconds. Range: 600 to 86400. Default: 3600. Recommended value: 600.</td>
</tr>
<tr>
<td></td>
<td>• min sec: (Optional) Minimum expiration time for a registration, in seconds. The range is from 60 to 3600. The default is 60.</td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exits SIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-serv-sip)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> exit</td>
<td>Exits voice-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> voice register global</td>
<td>Enters voice register global configuration mode to set parameters for all supported SIP phones in Unified SRST.</td>
</tr>
<tr>
<td>Example: Router(config)# voice register global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> default mode</td>
<td>Enables mode for provisioning SIP phones in Unified SRST. The default mode is Unified SRST itself.</td>
</tr>
<tr>
<td>Example: Router(config-register-global)# default mode</td>
<td></td>
</tr>
</tbody>
</table>
### Configure Unified SRST on Cisco 4000 Series Integrated Services Platform

**Step 14**

**max-dn max-directory-numbers**

**Example:**

```
Router(config-register-global)# max-dn 50
```

Limits number of directory numbers to be supported by this router.

- Maximum number is platform and version-specific. Type ? for value.

**Step 15**

**max-pool max-voice-register-pools**

**Example:**

```
Router(config-register-global)# max-pool 40
```

Sets maximum number of SIP phones to be supported by the Unified SRST router.

- Maximum number is platform and version-specific. Type ? for value.

**Step 16**

**exit**

**Example:**

```
Router(config-register-global)# exit
```

Exits voice register global configuration mode.

**Step 17**

**voice register pool pool-tag**

**Example:**

```
Router(config)# voice register pool 1
```

Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.

**Step 18**

**id { network address mask mask | ip address mask mask }**

**Example:**

```
Router(config-register-pool)# id network 10.64.88.0 mask 255.255.255.0
```

Explicitly identifies a locally available individual SIP phone to support a degree of authentication.

**Step 19**

**dtmf-relay rtp-npte**

**Example:**

```
Router(config-register-pool)# dtmf-relay rtp-npte
```

Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type and enables DTMF relay using the RFC 2833 standard method.

**Step 20**

**no vad**

**Example:**

```
Router(config-register-pool)# no vad
```

Disables voice activity detection (VAD) on the VoIP dial peer.

- VAD is enabled by default. Because there is no comfort noise during periods of silence, the call may seem to be disconnected. You may prefer to set no vad on the SIP phone pool.
Configure Voice Hunt Groups on Unified SRST

To redirect calls for a specific number (pilot number) to a defined group of directory numbers on Cisco Unified SCCP and SIP IP phones, perform the following steps.

Voice Hunt Group on Unified SRST is supported for Parallel, Sequential, Peer, and Longest-Idle hunt groups. Only the basic call features such as Call, Hold or Resume are supported for Unified SRST on Cisco 4000 Series Integrated Services Routers. For support of advanced features such as Auto Logout, Members Logout, and supplementary call features, you need to configure Unified E-SRST. For more information on Voice Hunt Group support on Unified E-SRST, see Unified E-SRST with Support for Voice Hunt Group, page 96.

For a list of restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers, see Restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers, page 37

Prerequisites

- Cisco IOS XE Denali 16.3.1 or later versions.
- Shared Lines are not supported on Unified SRST.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice hunt-group hunt-tag [longest-idle | parallel | peer | sequential]
4. pilot number [secondary number]
5. list number
6. final number
7. preference preference-order [secondary secondary-order]
8. timeout seconds

Example:
Router(config-register-pool)# codec g729r8

Step 22
end

Example:
Router(config-register-pool)# end

Command or Action | Purpose
---|---
**Step 21** codec codec-type [bytes] | Specifying the codec supported by a single SIP phone or a VoIP dial peer in a Cisco Unified SIP SRST environment. The codec-type argument specifies the preferred codec and can be one of the following:
- g711alaw: G.711 a–law 64,000 bps.
- g711ulaw: G.711 mu–law 64,000 bps.
- g729r8: G.729 8000 bps (default).
The bytes argument is optional and specifies the number of bytes in the voice payload of each frame.

**Step 22** end | Returns to privileged EXEC mode.
## Configure Voice Hunt Groups on Unified SRST

### 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 hunt-group **hunt-tag** [**longest-idle** | Enters voice hunt-group configuration mode to define a hunt group.  
  - **highest available**—Unique sequence number of the hunt group to be configured. Range is 1 to 100.  
  - **longest idle**—Hunt group in which calls go to the directory number that has been idle for the longest time.  
  - **parallel**—Hunt group in which calls simultaneously ring multiple phones.  
  - **peer**—Hunt group in which the first directory number is selected round-robin from the list.  
  - **sequential**—Hunt group in which directory numbers ring in the order in which they are listed, left to right.  
  - To change the hunt-group type, remove the existing hunt group first by using the **no** form of the command; then, recreate the group. |
| **Example:** Router(config)# voice hunt-group 1 longest-idle | |
| **Step 4** pilot **number** [**secondary number**] | Defines the phone number that callers dial to reach a voice hunt group.  
  - **number**—String of up to 16 characters that represents an E.164 phone number.  
  - Number string may contain alphabetic characters when the number is to be dialed only by the Unified SRST router, as with an intercom number, and not from phone keypads.  
  - **secondary number**—(Optional) Keyword and argument combination defines the number that follows as an additional pilot number for the voice hunt group.  
  - Secondary numbers can contain wildcards. A wildcard is a period (.), which matches any entered digit. |
| **Example:** Router(config-voice-hunt-group)# pilot number 8100 | |
### Command or Action

**Step 5**  
list number

**Example:**  
Router(config-voice-hunt-group)# list 8000, 8010, 8020, 8030

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a list of extensions that are members of a voice hunt group. To remove a list from a router configuration, use the no form of this command.</td>
</tr>
<tr>
<td>- number—List of extensions to be added as members to the voice hunt group. Separate the extensions with commas.</td>
</tr>
<tr>
<td>- Add or delete all extensions in a hunt-group list at one time. You cannot add or delete a single number in an existing list.</td>
</tr>
<tr>
<td>- There must be from 2 to 10 extensions in the hunt-group list, and each number must be a primary or secondary number.</td>
</tr>
<tr>
<td>- Any number in the list cannot be a pilot number of a parallel hunt group.</td>
</tr>
</tbody>
</table>

**Step 6**  
final number

**Example:**  
Router(config-voice-hunt-group)# final 8888

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the last extension in a voice hunt group.</td>
</tr>
<tr>
<td>- If a final number in one hunt group is configured as a pilot number of another hunt group, the pilot number of the first hunt group cannot be configured as a final number in any other hunt group.</td>
</tr>
</tbody>
</table>

**Step 7**  
preference preference-order [secondary secondary-order]

**Example:**  
Router(config-voice-hunt-group)# preference 6

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the preference order for the directory number associated with a voice hunt-group pilot number.</td>
</tr>
<tr>
<td>Note We recommend that the parallel hunt-group pilot number be unique in the system. Parallel hunt groups may not work if there are more than one partial or exact dial-peer match. For example, if the pilot number is “8000” and there is another dial peer that matches “8...”. If multiple matches cannot be avoided, give parallel hunt groups the highest priority to run by assigning a lower preference to the other dial peers. Note that 8 is the lowest preference value. By default, dial peers created by parallel hunt groups have a preference of 0.</td>
</tr>
<tr>
<td>- preference-order—Range is 0 to 8, where 0 is the highest preference and 8 is the lowest preference. Default is 0.</td>
</tr>
<tr>
<td>- secondary secondary-order—(Optional) Keyword and argument combination is used to set the preference order for the secondary pilot number. Range is 1 to 8, where 0 is the highest preference and 8 is the lowest preference. Default is 7.</td>
</tr>
</tbody>
</table>
Configure Voice Hunt Groups on Unified SRST

This section provides configuration information for some of the features supported on Unified SIP SRST.

Configure Feature Support on Unified SIP SRST

This section provides configuration information for some of the features supported on Unified SIP SRST.

Configure SIP-to-SIP Call Forwarding

SIP-to-SIP call forwarding (call routing) is available. Call forwarding is provided either by the phone or by using a back-to-back user agent (B2BUA), which allows call forwarding on any dial peer. Calls into a SIP device may be forwarded to other SIP or SCCP devices (including Cisco Unity, third-party voice-mail systems, or an auto attendant or IVR system such as IPCC and IPCC Express). In addition, SCCP IP phones may be forwarded to SIP phones.

Cisco Unity or other voice messaging systems connected by a SIP trunk or SIP user agent are able to pass a message-waiting indicator (MWI) when a message is left. The SIP phone then displays the MWI when indicated by the voice messaging system.

Note: SIP-to-H.323 call forwarding is not supported.

To configure SIP-to-SIP call forwarding, you must first allow connections between specific types of endpoints in a Cisco IP-to-IP gateway. The allow-connections command grants this capability. Once the SIP-to-SIP connections are allowed, you can configure call forwarding under an individual SIP phone pool. Any of the following commands can be used to configure call forwarding, according to your needs:

- Under voice register pool
  - call-forward b2bua all directory-number
– call-forward b2bua busy directory-number
– call-forward b2bua mailbox directory-number
– call-forward b2bua noan directory-number [timeout seconds]

In a typical Cisco Unified SIP SRST setup, the call-forward b2bua mailbox command is not used; however, it is likely to be used in a Cisco Unified SIP Communications Manager Express (CME) environment. Detailed procedures for configuring the call-forward b2bua mailbox command are found in the Cisco Unified Communications Manager (CallManager) documentation on Cisco.com.

The command call-forward b2bua all needs to point towards the trunk.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool tag
4. call-forward b2bua all directory-number
5. call-forward b2bua busy directory-number
6. call-forward b2bua mailbox directory-number
7. call-forward b2bua noan directory-number timeout seconds
8. 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>• 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>Step 3 voice register pool tag</td>
<td>Enters voice register pool configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Use this command to control which phone registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td>Step 4 call-forward b2bua all directory-number</td>
<td>Enables call forwarding for a SIP back-to-back user agent (B2BUA) so that all incoming calls are forwarded to another non-SIP station extension (that is, SIP trunk, H.323 trunk, SCCP device or analog/digital trunk).</td>
</tr>
<tr>
<td>Example:</td>
<td>• directory-number: Phone number to which calls are forwarded. Represents a fully qualified E.164 number. Maximum length of the phone number is 32.</td>
</tr>
<tr>
<td>Step 3 configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configure Voice Hunt Groups on Unified SRST

Configure Call Blocking Based on Time of Day, Day of Week, or Date

This section applies to both SCCP and SIP SRST. Call blocking prevents the unauthorized use of phones and is implemented by matching a pattern of up to 32 digits during a specified time of day, day of week, or date. Cisco Unified SIP SRST provides SIP endpoints the same time-based call blocking mechanism that is currently provided for SCCP phones. The call blocking feature supports all incoming calls, including incoming SIP and analog FXS calls.

Note
Pin-based exemptions and the “Login” toll-bar override are not supported in Cisco Unified SIP SRST.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5**
*call-forward b2bua busy directory-number* | Enables call forwarding for a SIP B2BUA so that incoming calls to a busy extension are forwarded to another extension. |
| **Example:**
Router(config-register-pool)# call-forward b2bua busy 5006 | |
| **Step 6**
*call-forward b2bua mailbox directory-number* | Controls the specific voice-mail box selected in a voice-mail system at the end of a call forwarding exchange. |
| **Example:**
Router(config-register-pool)# call-forward b2bua mailbox 5007 | |
| **Step 7**
*call-forward b2bua noan directory-number timeout seconds* | Enables call forwarding for a SIP B2BUA so that incoming calls to an extension that does not answer after a configured amount of time are forwarded to another extension. |
| **Example:**
Router(config-register-pool)# call-forward b2bua noan 5010 timeout 10 | This command is used if a phone is registered with a Cisco Unified SIP SRST router, but the phone is not reachable because there is no IP connectivity (there is no response to Invite requests). |
| **Step 8**
*end* | Returns to privileged EXEC mode. |
| **Example:**
Router(config-register-pool)# end | |

*directory-number:* Phone number to which calls are forwarded. Represents a fully qualified E.164 number. Maximum length of the phone number is 32.

*timeout seconds:* Duration, in seconds, that a call can ring with no answer before the call is forwarded to another extension. Range is 3 to 60000. The default value is 20.
The commands used for SIP phone call blocking are the same commands that are used for SCCP phones on your Cisco Unified SRST system. The Cisco SRST session application accesses the current after-hours configuration under call-manager-fallback mode and applies it to calls originated by Cisco SIP phones that are registered to the Cisco SRST router. The commands used in call-manager-fallback mode that set block criteria (time/date/block pattern) are the following:

- **after-hours block pattern** pattern-tag pattern [7-24]
- **after-hours day** day start-time stop-time
- **after-hours date** month date start-time stop-time

When a user attempts to place a call to digits that match a pattern that has been specified for call blocking during a time period that has been defined for call blocking, the call is immediately terminated and the caller hears a fast busy.

In SRST (call-manager-fallback configuration mode), there is no phone- or pin-based exemption to after-hours call blocking. However, in Cisco Unified SIP SRST (voice register pool mode), individual IP phones can be exempted from all call blocking using the **after-hours exempt** command.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. call-manager-fallback
4. **after-hours block pattern** tag pattern [7-24]
5. **after-hours day** day start-time stop-time
6. **after-hours date** month date start-time stop-time
7. exit
8. voice register pool tag
9. after-hour exempt
10. 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>Router&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:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</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 3</td>
<td><code>call-manager-fallback</code></td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config)# call-manager-fallback
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th><code>after-hours block pattern tag pattern [7-24]</code></th>
<th>Defines a pattern of outgoing digits to be blocked. Up to 32 patterns can be defined, using individual commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• If the 7-24 keyword is specified, the pattern is always blocked, 7 days a week, 24 hours a day.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the 7-24 keyword is not specified, the pattern is blocked during the days and dates that are defined using the <code>after-hours day</code> and <code>after-hours date</code> commands.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config-cm-fallback)# after-hours block pattern 1 91900
```

<table>
<thead>
<tr>
<th>Step 5</th>
<th><code>after-hours day day start-time stop-time</code></th>
<th>Defines a recurring time period based on the day of the week during which calls are blocked to outgoing dial patterns that are defined using the <code>after-hours block pattern</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• day: Day of the week abbreviation. The following are valid day abbreviations: sun, mon, tue, wed, thu, fri, sat.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• start-time stop-time: Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs on the day following the start time. For example, “mon 19:00 07:00” means “from Monday at 7 p.m. until Tuesday at 7 a.m.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config-cm-fallback)# after-hours day mon 19:00 07:00
```

<table>
<thead>
<tr>
<th>Step 6</th>
<th><code>after-hours date month date start-time stop-time</code></th>
<th>Defines a recurring time period based on month and date during which calls are blocked to outgoing dial patterns that are defined using the <code>after-hours block pattern</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• month: Month abbreviation. The following are valid month abbreviations: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• date: Date of the month. Range is from 1 to 31.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• start-time stop-time: Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. The stop time must be larger than the start time. The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router(config-cm-fallback)# after-hours date jan 1 00:00 00:00
```
Verification

To verify the feature’s configuration, enter one of the following commands:

- `show voice register dial-peer`: Displays all the dial peers created dynamically by phones that have registered. This command also displays configurations for after hours blocking and call forwarding.
- `show voice register pool <tag>`: Displays information about a specific pool.
- `debug ccsip message`: Debugs basic B2BUA calls.

For more information about these commands, see *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.
SIP Call Hold and Resume

Unified SRST supports the ability for SIP phones to place calls on hold and to resume from calls placed on hold. This also includes support for a consultative hold where A calls B, B places A on hold, B calls C, and B disconnects from C and then resumes with A. Support for call hold is signaled by SIP phones using “re-INVITE c=0.0.0.0” and also by the receive-only mechanism.

No configuration is necessary.

Configure Music On Hold for Unified SRST

Unified SRST supports the ability for SIP phones to play music for calls placed on hold. The following is the recommended configuration for Music On Hold (MOH) on a SIP Phone that falls back to Unified SRST.

SUMMARY STEPS

1. enable
2. configure terminal
3. no telephony-service
4. call-manager-fallback
5. moh enable-g711 "flash:filename"
6. moh g729 "flash:filename"
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> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no telephony-service</td>
<td>Removes all the configurations for IP phones configured under the telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# no telephony-service</td>
<td></td>
</tr>
</tbody>
</table>
Configure Voice Hunt Groups on Unified SRST

### Enabling KPML for SIP Phones

Perform the following steps to enable KPML digit collection on a SIP phone.

**Restrictions**

- A dial plan assigned to a phone has priority over KPML.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice register pool pool-tag
4. digit collect kpml
5. end
6. show voice register dial-peer

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>call-manager-fallback</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# call-manager-fallback</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>moh enable-g711 &quot;bootflash:filename&quot;</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# moh enable-g711 &quot;bootflash:music-on-hold.au&quot;</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>moh g729 &quot;bootflash:filename&quot;</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# moh g729 &quot;flash:SampleAudioSource.g729.wav&quot;</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# end</td>
</tr>
</tbody>
</table>
**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>Router&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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>voice register pool pool-tag</td>
<td>Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# voice register pool 4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>digit collect kpml</td>
<td>Enables KPML digit collection for the SIP phone.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-register-pool)# digit collect kpml</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-register-pool)# end</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>show voice register dial-peers</td>
<td>Displays details of all dynamically created VoIP dial peers associated with the Cisco Unified CME SIP register including the defined digit collection method.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# show voice register dial-peers</td>
<td></td>
</tr>
</tbody>
</table>

**Disabling SIP Supplementary Services for Call Forward and Call Transfer**

Perform the following steps to disable REFER messages for call transfers and redirect responses for call forwarding from being sent to the destination by Unified SRST. You can disable these supplementary features if the destination gateway does not support them.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
   or
   dial-peer voice tag voip
### 4. no supplementary-service sip {moved-temporarily | refer}

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: Router&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: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode to set global parameters for VoIP features.</td>
</tr>
<tr>
<td>or dial-peer voice tag voip</td>
<td>or</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td>Enters dial peer configuration mode to set parameters for a specific dial peer.</td>
</tr>
<tr>
<td>or Router(config)# dial-peer voice 99 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no supplementary-service sip {moved-temporarily</td>
<td>refer}</td>
</tr>
<tr>
<td>Example: Router(conf-voi-serv)# no supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td>or Router(config-dial-peer)# no supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# end</td>
<td></td>
</tr>
<tr>
<td>or Router(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

---

**Configuring Idle Prompt Status for SIP Phones**

Perform the following steps to customize the message that displays on SIP phones after the phones failover to Cisco Unified SRST.
You do not need to create new configuration files with the create profile command and restart the phones after changing the idle status message in Cisco Unified SRST. Modifying the status message takes effect immediately in Cisco Unified SRST.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice register global
4. system message string
5. end
6. show voice register global

**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> Router&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> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register global</td>
<td>Enters voice register global configuration mode to set global parameters for all supported SIP phones in a Cisco Unified CME environment.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice register global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> system message string</td>
<td>Defines a status message that displays on SIP phones registered to Cisco Unified SRST.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-global)# system message fallback active</td>
<td>• <em>string</em>: Up to 32 alphanumeric characters. Default is “CM Fallback Service Operating.”</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-global)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show voice register global</td>
<td>Displays all global configuration parameters associated with SIP phones.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show voice register global</td>
<td></td>
</tr>
</tbody>
</table>
Examples

The following are sample configurations for supporting SIP SRST on Cisco 4000 Series Integrated Services Router.

Example for Configuring Unified SIP SRST on Cisco 4000 Series Integrated Services Routers

The following example shows how to configure Unified SIP SRST on Cisco 4000 Series Integrated Services Routers.

```
! voice service voip
allow-connections sip to sip
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
supplementary-service media-renegotiate
sip
registrar server expires max 120 min 60
!
! voice register global
default mode
max-dn 40
max-pool 40
!
voice register pool 1
id network 8.55.0.0 mask 255.255.0.0
dtmf-relay rtp-nre
codec g711ulaw
no vad
!
!
```

Example for Configuring Voice Hunt Groups in Unified SIP SRST

The following example shows how to configure longest-idle hunt group 20 with pilot number 4701, final number 5000, and 6 numbers in the list. After a call is redirected six times (makes 6 hops), it is redirected to the final number 5000.

```
Router(config)# voice hunt-group 20 longest-idle
Router(config-voice-hunt-group)# pilot 4701
Router(config-voice-hunt-group)# list 4001, 4002, 4023, 4028, 4045, 4062
Router(config-voice-hunt-group)# final 5000
Router(config-voice-hunt-group)# hops 6
Router(config-voice-hunt-group)# timeout 20
Router(config-voice-hunt-group)# exit
```
Examples for Configuring IPv6 Pools for SIP IP Phones

The following example provides configuration of IPv6 pools for SIP IP Phones:

```plaintext
ipv6 unicast-routing
voice service voip
sip
no anat
call service stop
exit
exit
sip-ua
protocol mode dual-stack
exit
voice service voip
sip
no call service stop
exit
voice register global
default mode
max-dn 50
max-pool 40
exit
voice register pool 1
id network 2001:420:54FF:13::901:0/117
end
```

The following example provides interface configuration for IPv6 supported on Unified SRST:

```plaintext
configure terminal
interface GigabitEthernet0/0/1
ip address 10.64.86.229 255.255.255.0
negotiation auto
ipv6 address 2001:420:54FF:13::312:82/119
ipv6 enable
```

The following example provides IP route configuration for IPv6 supported on Unified SRST:

```plaintext
```

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

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

The following example displays output when SIP call service is active with the `no call service stop` CLI command:

```plaintext
Router# show sip-ua service
SIP Service is up
under 'voice service voip', 'sip' submode
```
Example for Configuring Call Blocking Based on Time of Day, Day of Week, or Date

The following example defines several patterns of digits for which outgoing calls are blocked. Patterns 1 and 2, which block calls to external numbers that begin with 1 and 011, are blocked on Monday through Friday before 7 a.m. and after 7 p.m. Pattern 3 blocks calls to 900 numbers 7 days a week, 24 hours a day.

call-manager-fallback
  after-hours block pattern 1 91
  after-hours block pattern 2 9011
  after-hours block pattern 3 91900 7-24
  after-hours day mon 19:00 07:00
  after-hours day tue 19:00 07:00
  after-hours day wed 19:00 07:00
  after-hours day thu 19:00 07:00
  after-hours day fri 19:00 07:00

The following example exempts a Cisco SIP phone pool from the configured blocking criteria:

voice register pool 1
  after-hour exempt

Example for Configuring Music On Hold for Unified SIP SRST

The following example shows how to configure Music On Hold (MOH) for Unified SIP SRST on Cisco 4000 Series Integrated Services Routers.

enable
configure terminal
no telephony-service
call-manager-fallback
moh enable-g711 "flash:music-on-hold.au"
moh g729 "flash:SampleAudioSource.g729.wav"

Example for Configuring SIP-to-SIP Call Forwarding on Unified SRST

The following is a sample configuration for SIP-to-SIP Call Forwarding on Unified SRST.

enable
configure terminal
voice register pool 15
call-forward b2bua busy 5006
call-forward b2bua mailbox 5007
call-forward b2bua noan 5010 timeout 8

Example for Configuring Idle Prompt Status for SIP Phones

The following is a sample configuration for idle prompt status for SIP phones on Unified SRST.

enable
configure terminal
voice register global
system message fallback active
end
Example for Disabling SIP Supplementary Services for Call Forward and Call Transfer

The following is a sample configuration for disabling SIP supplementary services for call forward and call transfer on Unified SRST.

```
enable
configure terminal
voice service voip
no supplementary-service sip {moved-temporarily | refer}
end
```
Cisco Unified Enhanced Survivable Remote Site Telephony

This chapter describes the Unified Enhanced Survivable Remote Site Telephony (Unified E-SRST) feature which is an enhancement of the SRST feature that provides advanced services compared to the classic Unified SRST.

Contents

- Migration from Unified SRST Manager to Unified E-SRST, page 95
- Unified E-SRST with Support for Voice Hunt Group, page 96
- SIP: Configure Unified E-SRST, page 99
- SCCP: Configure Unified E-SRST, page 115
- Configure Digest Credentials On Unified Communications Manager, page 121
- Unified E-SRST Scale Support, page 122
- Where to Go Next, page 123

Migration from Unified SRST Manager to Unified E-SRST

Cisco Unified Survivable Remote Site Telephony Manager is End-of-Life (EOL). Hence, provisioning for Unified E-SRST through Unified SRST Manager is not supported for Unified E-SRST Release 12.2 and later releases. Unified E-SRST is provisioned only using CLI commands (manual provisioning) to support fail back of phones registered to Unified Communications Manager. For more information on configuring Unified E-SRST, see SIP: Configure Unified E-SRST, page 99 and SCCP: Configure Unified E-SRST, page 115. For information on Cisco Unified Survivable Remote Site Telephony Manager End-of-Life announcement, see Cisco Unified Survivable Remote Site Telephony Manager Product Bulletin.

Unified SRST Manager is a GUI-based tool that helps to monitor, report, and troubleshoot remote sites. It performs automatic sync up between the Unified Communications Manager and the Unified E-SRST gateway that helps in adding, deleting, and modifying the users and phones including dial-plan mapping. It also provides centralized management and control of all remote sites. For more information on the Unified SRST Manager that is End-of-Life, see Administration Guide for Cisco Unified SRST Manager.
Benefits of Unified-ESRST

When you configure Unified E-SRST, it provides the following feature benefits in comparison to the classic Unified SRST:

- Voice Hunt Group
  - Shared Lines
  - Mixed Shared Lines (SIP and SCCP Phones)
  - Hunt Statistics Collection
  - Mixed Deployment (SIP and SCCP Phones)
- Shared Line
- BLF
- Video
- B-ACD

For more information on configuring VHG with Unified E-SRST, see Unified E-SRST with Support for Voice Hunt Group, page 96. For more information on configuring Shared Line, BLF, and Video with Unified E-SRST, see SIP: Configure Unified E-SRST, page 99.

Toll Fraud Prevention for SIP Line Side on Unified E-SRST

Unified E-SRST Release 12.6 enhances the existing Toll Fraud Prevention feature by enforcing security on the SIP line side of Unified E-SRST. The feature enhancement secures the Unified E-SRST system against potential toll fraud exploitation by unauthorized users from the SIP line side.

The configuration and characteristics of toll fraud prevention offered on the SIP line side of Unified E-SRST is same as the support available on Unified SRST. For more information on the feature, see Toll Fraud Prevention for SIP Line Side on Unified SRST, page 60.

Unified E-SRST with Support for Voice Hunt Group

From Unified E-SRST Release 12.2, support is introduced for Voice Hunt Group with Cisco Unified Enhanced Survivable Remote Site Telephony (Unified E-SRST). The deployment is supported on SIP and SCCP phones. The Cisco IP Phone 7800 and 8800 Series are the SIP phones supported for this deployment. The Unified E-SRST deployment for voice hunt group enhancement is introduced on the Cisco 4000 Series Integrated Services Routers.

As part of the enhancement, voice hunt group features are supported in the E-SRST mode. Voice hunt group deployments with Sequential, Parallel, Longest Idle, and Peer call blasting is supported with Unified E-SRST 12.2 and onwards.

During a WAN outage, the SIP phones on the Cisco Unified Communications Manager (Unified Communications Manager) fall back to Unified E-SRST router in mode esrst. The SIP phones are logged in to the hunt group by default in this scenario. However, if the CLI command members logout is configured under the voice hunt group configuration mode, the phones will be in logged out state. In the Unified E-SRST mode, the phone that falls back on Unified E-SRST can toggle state and log in (or log out) to the voice hunt group using HLog via Feature Access Code (FAC). The DN status (logged in or logged out) is displayed on the phones registered with Unified E-SRST. The following FAC codes are available as part of the enhancement introduced on Unified E-SRST:
When the user inputs FAC from a phone with multiple lines, the log out behavior is known to be different across a deployment with common voice register pool configuration and individual voice register pool configuration.

- **Common Voice Register Pool Configuration** — The DN's log out individually, and not at the phone level.
- **Individual Voice Register Pool Configuration** — The DN's log out at the phone level, irrespective of the DN (primary, secondary, and so on) from which FAC input was provided by the user.

When the WAN is available, the phones register back with Unified Communications Manager. For a sample configuration of Unified E-SRST with voice hunt group enhancements, see [Example for configuring Unified E-SRST with Voice Hunt Group Enhancements](#), page 110.

The Unified E-SRST 12.2 Release introduces support for voice hunt group with shared lines and mixed shared lines (SCCP and SIP phones). For a mixed shared line supported with voice hunt group, only individual voice register pools can be configured. Common voice register pools are not supported. For a sample configuration of mixed shared lines configured for a voice hunt group on Unified E-SRST, see [Example for Configuring Shared Line with Voice Hunt Group on Unified E-SRST](#), page 112.

Also, hunt statistic collection is supported for Unified E-SRST 12.2 and later releases.

A mixed deployment of SIP and SCCP phones is supported on Unified E-SRST, Release 12.2. Hunt Group Logout from a mixed deployment of SIP and SCCP phones is supported using:

- FAC
- Feature Button, or
- DND

Line level logout and phone level logout is supported using FAC (*4).

**Note**

Hunt Group logout is not supported for shared lines. Shared lines retain their logged in status.

### Support for B-ACD in Unified E-SRST

B-ACD is supported as part of the Unified E-SRST enhancement introduced in Release 12.2. For SIP phones that fall back to Unified E-SRST router in `mode esrst`, you need to ensure that the CLI command `members logout` is configured. The Members Logout functionality handles login back from the phones using FAC. It also supports call delivery to Voice Hunt Group from B-ACD.

For a sample configuration, see [Example for Configuring B-ACD with Unified E-SRST](#), page 111.

### Recommendations for Configuring Voice Hunt Group on Unified E-SRST

The Unified E-SRST Release with Support for voice hunt group has the following design characteristics:
• For all the directory numbers falling back from Unified Communications Manager, a common voice register pool configuration as well as an individual voice register pool configuration is supported for this deployment. An individual voice register pool configured with the CLI command `id device-id-name`, along with `voice register dn` configuration, is recommended.

• Ensure that the CLI command `mode esrst` is configured under `voice register global` configuration mode for phones to fall back to Unified E-SRST.

• Ensure that the CLI command `id ip` or `id device-id-name` is configured under `voice register pool` configuration mode, along with `voice register dn` configuration, for a deployment with individual voice register pool configuration. For a sample configuration, see Example for configuring Unified E-SRST with Voice Hunt Group Enhancements, page 110.

• Ensure that the CLI command `id device-id-name` is preferred over `id ip` as the CLI command to configure under `voice register pool` configuration mode in scenarios where the IP address of the phone might change due to the DHCP configured on the phone.

• Ensure that the CLI command `id network` is configured under `voice register pool` configuration mode for a deployment with common voice register pool configuration. The recommended configuration is `id network 8.55.0.0 255.255.0.0` so as to facilitate registration of phones falling back on Unified E-SRST from Unified Communications Manager.

• Ensure that the CLI command `members logout` is configured under `voice hunt-group` configuration mode. The CLI is applied by default when the SIP phones fall back to Unified E-SRST from Unified Communications Manager.

• Ensure that the CLI command `fac standard` is configured under `telephony-service` configuration mode. If you want to configure a FAC code other than *5, you need to configure the CLI command `fac custom` under `telephony-service` configuration mode.

• Ensure that the CLI commands `call-park system application` and `hunt-group logout hlog` are configured under `telephony-service` configuration mode. The CLI commands are mandatory configuration for FAC functionality to work.

For steps on configuring voice hunt groups on Unified E-SRST, see Configure Voice Hunt Groups on Unified E-SRST, page 108.

For a sample configuration of voice hunt groups on Unified E-SRST, see Example for configuring Unified E-SRST with Voice Hunt Group Enhancements, page 110.

Restrictions for Unified E-SRST, Release 12.2

The Unified E-SRST deployment with voice hunt group is known to have the following restrictions:

• Auto Logout is not supported
• Programmable Line Keys (PLK) are not supported
• HLog Softkey is not supported

Note

The existing support for Cisco Jabber is now End of Life (EOL). Hence, Cisco Jabber is not supported on Unified SRST, E-SRST.
SIP: Configure Unified E-SRST

The Enhanced SRST for Cisco Unified SIP IP Phones feature supports version negotiation between the SIP phones and ESRST to enable more features in the Cisco Unified ESRST mode. In the current scenario, when the SIP phones fall back to the SRST mode, features such as Shared-Line, Busy-Lamp-Field (BLF), and Video call are disabled on the phones because the features are not supported in the SRST mode. However, with the Enhanced Survivable Remote Site Telephony (E-SRST) deployment, you can enable the basic and supplementary call features. Also, you can enable the following features using version negotiation:

- Shared-Line
- Busy-Lamp-Field (BLF)
- Video Calls

Table 3-1 contains a list of supported features and the expected behavior of the features in the E-SRST mode.

Table 3-1  Supported features in the E-SRST mode

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported Features</th>
<th>Expected Behavior in the E-SRST Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared-Line</td>
<td>cBarge</td>
<td>Not Supported (After the failover, the phone does not retain the key.)</td>
</tr>
<tr>
<td></td>
<td>Privacy-on-hold</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Transfer</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Conference</td>
<td>Supported</td>
</tr>
<tr>
<td>BLF</td>
<td>BLF dn monitoring</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>BLF device-based</td>
<td>Not supported (Not supported in RT phones)</td>
</tr>
<tr>
<td></td>
<td>monitoring</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>BLF call-list</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring of Call-park</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>slot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring of Paging</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>dn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Monitoring of Conference</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>dn</td>
<td></td>
</tr>
</tbody>
</table>

- To enable version negotiation feature between ESRST & phone, user needs to configure "mode esrst" under voice register global mode.
- It is recommended to use SRST manager to automate the CLI provisioning of ESRST branch routers.

For more information on SRST, see the Cisco Unified SRST Manager Administration Guide.
Restrictions

- The Version Negotiation feature is supported only on the Cisco Unified 9951, 9971, 8961 SIP IP phones, Cisco IP Phone 7800 and 8800 Series.
- The phone firmware version should be Version 9.4.1 or later versions.
- This feature supports video calls only between the local Cisco Unified SIP IP phones and the No Time-Division Multiplexing (TDM) video calls during the SRST failovers.
- To enable phone specific features like shared-line & BLF work, individual voice register pools need to be configured.

Enable the E-SRST Mode

To enable the version negotiation feature in the Unified E-SRST mode, perform the following procedure.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register global
4. mode esrst
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 the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
</tbody>
</table>
| **Example:**
  Router> enable | |
| **Step 2** configure terminal | Enters the global configuration mode. |
| **Example:**
  Router# configure terminal | |
| **Step 3** voice register global | Enters the voice register global configuration mode to set the parameters for all the supported SIP phones in Cisco Unified CME. |
| **Example:**
  Router(config)# voice register global | |
| **Step 4** mode esrst | Configures the E-SRST mode under the voice register global mode. |
| **Example:**
  Router(config-register-global)# mode esrst | |
| **Step 5** exit | Exits the voice register-global configuration mode. |
| **Example:**
  Router(config-register-global)# exit | |

Configure SIP shared-line

To configure SIP shared-line, perform the following procedure:

1. enable
2. configure terminal
3. voice register dn \texttt{dn-tag}
4. number \texttt{number}
5. shared-line [max-calls \texttt{number-of-calls}]
6. huntstop channel \texttt{number-of-channels}
7. end

Configure BLF

To configure BLF, perform the following procedure:

1. enable
2. configure terminal
3. sip-ua
4. presence enable
5. exit
Enable a SIP Directory Number to be Watched

To enable a directory number to be watched, perform the following procedure:

1. `voice register dn dn-tag`
2. `number number`
3. `allow watch`
4. `end`

Enable BLF on a Voice Register Pool

To enable BLF on a `voice register pool`, perform the following steps:

1. `enable`
2. `configure terminal`
3. `voice register pool pool-tag`
4. `number tag dn dn-tag`
5. `blf-speed-dial tag number label str [device]`
6. `presence call-list` (To enable Presence feature for all the missed/received/placed calls)
7. `end`

For configuration information, see the *Cisco Unified Communications Manager Administration Guide*.

**Example: ESRST mode**

The following example shows how to enable the E-SRST mode:

```bash
Router# configure terminal
Router(config)# voice register global
Router(config-register-global)# mode esrst
```

**Example: Configuring Shared Line**

The following example shows how to configure shared-line:

```bash
Router(config)#voice register dn 1
Router (config-register-dn)#number 1111
Router (config-register-dn)#shared-line max-calls 7

Router(config)#voice register pool 1
Router(config-register-pool)#Id mac 002D.264E.54FA
Router(config-register-pool)#type 9971
Router(config-register-pool)#number 1 dn 1

Router(config)#voice register pool 2
Router(config-register-pool)#id mac 000D.39F9.3A58
```
Example: Configuring BLF

The following example shows how to configure BLF:

Router(config)\#voice register dn 1
Router (config-register-dn)\#number 1111
Router (config-register-dn)\#allow watch

Router(config)\#voice register dn 1
Router (config-register-dn)\#number 2222

Router(config)\#voice register pool 1
Router(config-register-pool)\#id mac 0015.6247.EF90
Router(config-register-pool)\#type 7971
Router(config-register-pool)\#number 1 dn 1

Router(config)\#voice register pool 2
Router(config-register-pool)\#id mac 0012.0007.8D82
Router(config-register-pool)\#type 7912
Router(config-register-pool)\#number 1 dn 2
Router(config-register-pool)\#blf-speed-dial 1 1111 label "1111"

Note
If the phone and the Unified E-SRST router are in different subnets and you are using \texttt{id mac} in the \texttt{voice register pool} configuration mode, then the user must configure digest credentials on Unified Communications Manager, and username password configuration under \texttt{voice register pool} on Unified E-SRST. Digest Configuration is not required with the \texttt{id device-id-name} CLI command introduced in Unified SRST Release 12.2.

Configure Unified E-SRST

The \texttt{mode esrst} under \texttt{telephony-service} and \texttt{voice register global} configuration mode provisions SCCP and SIP phones respectively to enable the enhanced services in Unified E-SRST mode. While Unified SRST supports only the basic voice hunt group features, Unified E-SRST supports advanced voice hunt group features such as HLog, shared lines, and B-ACD. To configure the basic Unified E-SRST, perform the following procedure:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. mode esrst
5. max-ephones max-phones
6. max-dn max-directory-numbers
7. ip source-address ip-address [port port] [any-match | strict-match]
8. call-park system application
9. hunt-group logout HLog
10. transfer-system full-consult
11. transfer-pattern transfer-pattern
12. fac standard
13. create cnf-files
14. exit
15. voice register global
16. mode esrst
17. max-dn max-directory-numbers
18. max-pool max-phones
19. exit
20. voice register dn dn-tag
21. number number
22. exit
23. voice register pool pool-tag
24. id [network address mask mask | ip address mask mask | device-id-name devicename]
25. dtmf-relay rtp-npe
26. exit
### 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 the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>mode esrst</td>
<td>Configures the E-SRST mode under the telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>max-ephones max-phones</td>
<td>Configures the maximum number of IP phones that can be supported by the router. The default is 0.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# max-ephones 40</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>max-dn max-directory-numbers</td>
<td>Sets the maximum number of directory numbers (DNs) that can be supported by the router.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>max-directory-numbers</em>: Maximum number of directory numbers (DNS) or virtual voice ports supported by the router. The maximum number is platform-dependent. The default is 0.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# max-dn 15</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>ip source-address ip-address [port port] [any-match</td>
<td>strict-match]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# ip source-address 8.39.23.24 port 2000</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>call-park system (application</td>
<td>redirect)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>application</em> — Enables the Call Park features supported in Unified SRST.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# call-park system application</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 9</strong> hunt-group logout {DND</td>
<td>HLog}</td>
<td>Sets the hunt-group logout options with Hlog in telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# hunt-group logout HLog</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> transfer-system full-consult</td>
<td>Specifies the call transfer method.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# transfer-system full-consult</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> transfer-pattern transfer-pattern</td>
<td>Allows transfer of telephone calls by Cisco Unified IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# transfer-pattern .T</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> fac { standard</td>
<td>custom { alias alias-tag</td>
<td>feature } }</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# fac standard</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> create cnf-files</td>
<td>Builds the eXtensible Markup Language (XML) configuration files that are required for IP phones, in telephony-service configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# create cnf-files version-stamp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> exit</td>
<td>Exits the telephony-service configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> voice register global</td>
<td>Enters the voice register global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# voice register global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> mode esrst</td>
<td>Configures the E-SRST mode under the voice register global mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# mode esrst</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> max-dn max-directory-numbers</td>
<td>Sets the maximum number of SIP phone directory numbers (extensions) that are supported by a Cisco router in voice register global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# max-dn 40</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>
</table>
| 18   | max-pool max-phones | Sets maximum number of SIP phones to be supported by the Unified SRST router.  
   | Example: Router(config-register-global)# max-pool 40 | - Version- and platform-dependent; type ? for range. |
| 19   | exit              | Exits the voice register global configuration mode. |
| 20   | voice register dn dn-tag | Enters voice register dn configuration mode to define a directory number for a SIP phone.  
   | Example: Router(config)# voice register dn 17 | The voice register dn configured in Unified E-SRST must be the same directory number (dn) configured in Unified Communications Manager. |
| 21   | number number     | Defines a valid number for a directory number. |
| 22   | exit              | Exits the voice register dn configuration mode. |
| 23   | voice register pool pool-tag | Enters the voice register pool configuration mode to set phone-specific parameters for a SIP phone. |
| 24   | id [{network address mask mask | ip address mask mask | mac address}] [device-id-name devicename] | Explicitly identifies a locally available individual or set of SIP IP phones. The keywords and arguments are defined as follows:  
   | Example: Router(config-register-pool)# id network 8.55.0.0 mask 255.255.0.0 | - **network address mask mask**: The network address mask keyword/argument combination is used to accept SIP Register messages for the indicated phone numbers from any IP phone within the indicated IP subnet.  
   | | - **ip address mask mask**: The ip address mask mask keyword/argument combination is used to identify an individual phone.  
   | | - **mac address**: MAC address of a particular Cisco Unified IP Phone.  
   | | - **device-id-name devicename**: Defines the device name to be used to download the phone’s configuration file. |
Configure Voice Hunt Groups on Unified E-SRST

To configure Voice Hunt Group feature on Unified E-SRST, perform the following procedure:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice hunt-group hunt-tag {longest-idle | parallel | peer | sequential}
4. members logout (optional)
5. list number [, number...]
6. timeout seconds
7. statistics collect
8. pilot 111

---

**Command or Action**

**Step 25**

dtmf-relay rtp-n.te

**Example:**

Router(config-register-pool)# dtmf-relay rtp-n.te

**Purpose**

Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type and enables DTMF relay using the RFC 2833 standard method.

**Step 26**

exit

**Example:**

Router(config-register-pool)# exit

**Purpose**

Exits the voice register pool configuration mode.

---

**Configure Voice Hunt Groups on Unified E-SRST**

To configure Voice Hunt Group feature on Unified E-SRST, perform the following procedure:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice hunt-group hunt-tag {longest-idle | parallel | peer | sequential}
4. members logout (optional)
5. list number [, number...]
6. timeout seconds
7. statistics collect
8. pilot 111

---

**Command or Action**

**Step 25**

dtmf-relay rtp-n.te

**Example:**

Router(config-register-pool)# dtmf-relay rtp-n.te

**Purpose**

Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type and enables DTMF relay using the RFC 2833 standard method.

**Step 26**

exit

**Example:**

Router(config-register-pool)# exit

**Purpose**

Exits the voice register pool configuration mode.
## 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 the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice hunt-group hunt-tag (longest-idle</td>
<td>sequential)</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice hunt-group 1 sequential</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> members logout</td>
<td>(optional) Configures a Unified SRST system for all non-shared static members or agents in a voice hunt group with the Hlogout initial state.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-voice-hunt-group)# members logout</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> list number [, number...]</td>
<td>Defines a list of extensions that are members of a voice hunt group.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-voice-hunt-group)# list 1812, 1813, 1814</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> timeout seconds</td>
<td>Defines the number of seconds after which a call that is not answered is redirected to the next number in a voice hunt-group list.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-voice-hunt-group)# timeout 30</td>
<td></td>
</tr>
</tbody>
</table>
Example for configuring Unified E-SRST with Voice Hunt Group Enhancements

The following is a sample configuration for Unified E-SRST Release 12.2 under `telephony-service`, `voice register global`, `voice register pool`, and `voice hunt-group` configuration modes, for a deployment with common voice register pool configuration.

```
Router#
telephony-service
call-park system application
hunt-group logout HLog
transfer-system full-consult
fac standard
Router#sh run | sec global
voice register global
mode esrst
max-dn 40
max-pool 40

Router# voice register pool 1
id network 8.55.0.0 mask 255.255.0.0
dtmf-relay rtp-nte
Router#
telephony-service
max-ephones 40
max-dn 50
ip source-address 8.39.23.24 port 2000
call-park system application
transfer-system full-consult
transfer-pattern .T
fac standard
create cnf-files version-stamp Jan 01 2002 00:00:00

Router#sh run | sec hunt
voice hunt-group 1 sequential
members logout
list 1812,1813,1814
timeout 30
statistics collect
pilot 1111
```

The following is a sample configuration for Unified E-SRST Release 12.2, for a deployment with individual voice register pool configuration, with the CLI command `id ip` configured.

```
Step 7
command or action:
Example:
Router(config-voice-hunt-group)# statistics collect

Step 8
exit
Example:
Router(config-voice-hunt-group)# exit
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>statistics collect</code></td>
<td>Enables the collection of call statistics for a voice hunt group.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits the voice hunt group configuration mode.</td>
</tr>
</tbody>
</table>

Example:
```
Router(config-voice-hunt-group)# statistics collect

Enables the collection of call statistics for a voice hunt group.
```

```
Router(config-voice-hunt-group)# exit

Exits the voice hunt group configuration mode.
```
The following is a sample configuration for Unified E-SRST Release 12.2, for a deployment with individual voice register pool configuration, with the CLI command `id device-id-name` configured.

```plaintext
voice register dn  2
  number 4000
!
voice register dn  3
  number 4002
!
voice register pool  2
  busy-trigger-per-button 2
  id device-id-name SEP00EBD5CD77ED
  type 8811
  number 1 dn 2
dtmf-relay rtp-nte
codec g711ulaw
!
voice register pool  3
  busy-trigger-per-button 2
  id device-id-name SEP0076861A7EDC
  type 7861
  number 1 dn 3
dtmf-relay rtp-nte
codec g711ulaw
```

**Example for Configuring B-ACD with Unified E-SRST**

The following is a sample configuration for B-ACD functionality supported with Unified E-SRST:

```plaintext
application
service aa-bcd bootflash:/app-b-acd-aa-3.0.0.4_thd_v4.tcl
paramspace english index 0
param second-greeting-time 60
param welcome-prompt _bacd_welcome.au
param call-retry-timer 8
param voice-mail 1811
paramspace english language en
param max-time-call-retry 16
```
Example for Configuring Shared Line with Voice Hunt Group on Unified E-SRST

The following is a sample configuration of Unified E-SRST, Release 12.2 with support for mixed shared lines (SIP and SCCP Phones) in a voice hunt group deployment.

Router# sh run | sec global
voice register global
  mode esrst
  no allow-hash-in-dn
  max-dn 40
  max-pool 40

Router# sh run | sec pool
  max-pool 40
voice register pool 1
  busy-trigger-per-button 2
  id device-id-name SEP00CCPC4AA4DC
type 8811
  number 1 dn 1
  number 2 dn 21
dtmf-relay rtp-nte
  username xxxx password uvwx
  codec g711ulaw
  no vad
voice register pool 2
  busy-trigger-per-button 2
  id device-id-name SEP00CCPC177A4E
type 8841
number 1 dn 2
dtmf-relay rtp-nte
username xxxx password uvwx
codec g711ulaw
no vad
voice register pool 3
busy-trigger-per-button 2
id device-id-name SEP0076861ADEF0
type 7841
number 1 dn 3
number 2 dn 22
dtmf-relay rtp-nte
username xxxx password uvwx
codec g711ulaw
no vad
voice register pool 4
busy-trigger-per-button 2
id device-id-name SEP00EBD5CD270C
type 8811
number 1 dn 4
number 2 dn 22
dtmf-relay rtp-nte
username xxxx password uvwx
codec g711ulaw
no vad
voice register pool 5
busy-trigger-per-button 2
id device-id-name SEP94D4692A2553
type 8841
number 1 dn 5
dtmf-relay rtp-nte
username xxxx password uvwx
codec g711ulaw
no vad
voice register pool 6
busy-trigger-per-button 2
id device-id-name SEP00CAE540C4B5
type 8811
number 1 dn 6
number 2 dn 21
dtmf-relay rtp-nte
username xxxx password uvwx
codec g711ulaw
no vad
alias exec pool show voice register pool all br

Router# sh run | sec dn
no allow-hash-in-dn
max-dn 40
voice register dn 1
voice-hunt-groups login
number 1811
voice register dn 2
voice-hunt-groups login
number 1812
voice register dn 3
voice-hunt-groups login
number 1813
voice register dn 4
voice-hunt-groups login
number 1814
voice register dn 5
voice-hunt-groups login
number 1815
voice register dn  6
   voice-hunt-groups login
number 1816
voice register dn  21
   voice-hunt-groups login
number 1821
   shared-line
voice register dn  22
   voice-hunt-groups login
number 1822
   shared-line

Router# sh run | sec ephone
max-ephones 40
ephone-dn  11
   number 1911
ephone-dn  12
   number 1912
ephone-dn  13
   number 1913
ephone-dn  14
   number 1914
ephone-dn  21
   number 1921
ephone-dn  22
   number 1822
   shared-line sip
ephone  11
   device-security-mode none
   mac-address 1111.1111.1911
   feature-button 1 HLog
type 7970
   button  1:11
ephone  12
   device-security-mode none
   mac-address 1111.1111.1912
   feature-button 1 HLog
type 7970
   button  1:12 2:21
ephone  13
   device-security-mode none
   mac-address 1111.1111.1913
   feature-button 1 HLog
type 7970
   button  1:13 2:21
ephone  14
   device-security-mode none
   mac-address 1111.1111.1914
   feature-button 1 HLog
type 7970
   button  1:14 2:22
alias ephone show ephone summary brief
alias exec ephone show ephone summary brief

Router# sh run | sec tele
telephony-service
   conference transfer-pattern
   mode erst
max-ephones 40
max-dn 50
ip source-address 8.39.23.24 port 2000
service phone sshAccess 0
SCCP: Configure Unified E-SRST

You need to configure mode esrst under telephony-service to enable ESRST mode for SCCP Phones.

Prerequisites

- Cisco Unified CME 10.5 or later version
- The telephony-services command must be configured

**Note**

For SCCP phones, CME-as-SRST mode is provisioned using the `srst mode auto-provision` command. From 10.5 release onwards, this command will be deprecated. When you try to configure CME-as-SRST mode, the following message will be displayed:

“Note: This configuration is being deprecated. Please configure "mode esrst" to use the enhanced SRST mode”.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `mode esrst`
5. `max-ephones max-phones`
6. `max-dn max-directory-numbers [preference preference-order] [no-reg primary | both]`
7. `ip source-address ip-address port port [any-match | strict-match]`
8. `exit`
9. `ephone-dn dn-tag [dual-line]`
10. `number number [secondary number] [no-reg [both | primary]]`
11. `name name`
12. `exit`
13. `ephone phone-tag`
14. `mac-address [mac-address]`
15. `type phone-type [addon 1 module-type [2 module-type]]`
16. `button button-number{separator}dn-tag [dn-tag...] [button-number{x}overlay-button-number]` [button-number...]
17. end
# Unified E-SRST with Support for Voice Hunt Group

## 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 the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# 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>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mode esrst</td>
<td>Configures the E-SRST mode under the telephony-service mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# mode esrst</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> max-ephones max-phones</td>
<td>Sets the maximum number of phones that can register to Unified E-SRST.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# max-ephones 24</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 6** max-dn max-directory-numbers [preference preference-order] [no-reg primary | both] Limits number of directory numbers to be supported by this router.
| Example:                  |                                                                         |
| Router(config-telephony)# max-dn 24 no-reg primary |                                                           |
| **Step 7** ip source-address ip-address [port port] [any-match | strict-match] Identifies the IP address and port number that the Unified SRST router uses for IP phone registration.  |
| Example:                  |                                                                         |
| Router(config-telephony)# ip source-address 192.168.11.1 port 2000 |                                                 |
| **Step 8** exit           | Exits telephony-service configuration mode.                             |
| Example:                  |                                                                         |
| Router(config-telephony)# exit |                                                               |
### Unified E-SRST with Support for Voice Hunt Group

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td><strong>ephone-dn dn-tag [dual-line]</strong></td>
<td>Enters ephone-dn configuration mode to define a directory number for an IP phone, intercom line, voice port, or a message-waiting indicator (MWI).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config)# ephone-dn 1</td>
</tr>
<tr>
<td>10</td>
<td><strong>number number [secondary number] [no-reg [both primary]]</strong></td>
<td>Associates an extension number with this directory number.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config-ephone-dn)# number 1001</td>
</tr>
<tr>
<td>11</td>
<td><strong>name name</strong></td>
<td>(Optional) Associates a name with this directory number.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config-ephone-dn)# name Smith, John</td>
</tr>
<tr>
<td>12</td>
<td><strong>exit</strong></td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config-telephony)# end</td>
</tr>
<tr>
<td>13</td>
<td><strong>ephone phone-tag</strong></td>
<td>Enters ephone configuration mode to set ephone specific parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config)# ephone 1</td>
</tr>
<tr>
<td>14</td>
<td><strong>mac-address [mac-address]</strong></td>
<td>Associates the MAC address of a Cisco IP phone with an ephone configuration in a Unified E-SRST system.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config-ephone)# mac-address 0022.555e.00f1</td>
</tr>
<tr>
<td>15</td>
<td><strong>type phone-type [addon 1 module-type [2 module-type]]</strong></td>
<td>Specifies the type of phone.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config-ephone)# type 7960</td>
</tr>
</tbody>
</table>
Example: Enhanced SRST mode configuration

The following example shows the status of the device in E-SRST mode:

```plaintext
show telephony-service
CONFIG (Version=10.5)
===================== 
Version 10.5 
Max phoneload sccp version 17 
Max dspfarm sccp version 18 
Cisco Unified Enhanced SRST
```

**Note** For SCCP phones, switching the mode from CME to ESRST and vice versa, results in wiping out the entire CME or ESRST configurations (including ephone, DNs, templates etc.).

Configure Mixed Shared Lines with SCCP Phones

To configure mixed shared lines between SCCP and SIP IP Phones on Unified E-SRST, perform the following procedure:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone-dn dn-tag [dual-line]`
4. `number number [secondary number] [no-reg [both | primary]]`
5. `shared-line sip`
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 the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the 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></td>
<td></td>
</tr>
<tr>
<td><code>ephone-dn dn-tag [dual-line]</code></td>
<td>Enters ephone dn configuration mode to define a directory number for an IP phone, intercom line, voice port, or a message-waiting indicator (MWI).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ephone-dn 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`number number [secondary number] [no-reg [both</td>
<td>primary]]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ephone-dn)# number 1001</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>shared-line sip</code></td>
<td>Adds an ephone-dn as a member of a shared directory number for a mixed shared line between Unified SIP and Unified SCCP IP phones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ephone-dn)# shared-line sip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-ephone-dn)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configure BLF for SCCP Phones

1. `enable`
2. `configure terminal`
3. `presence`
4. `max-subscription number`
5. `presence call-list` (To enable Presence feature for all the missed/received/placed calls)
6. `end`

### Enable an SCCP Directory Number to be Watched

To enable a directory number to be watched, perform the following procedure:

1. `ephone-dn dn-tag`
Enable BLF on an Ephone

To enable BLF on an ephone, perform the following steps:
1. enable
2. configure terminal
3. ephone ephone-tag
4. button button-number{separator}dn-tag [.dn-tag...] [button-number{x}overlay-button-number] [button-number...]
5. blf-speed-dial tag number label string [device]
6. presence call-list (To enable Presence feature for all the missed/received/placed calls)
7. end

Configure Digest Credentials On Unified Communications Manager

To configure the username and password with Digest Authentication on Unified Communications Manager, perform the following steps:

**Step 1**
Login to Cisco Unified Communications Manager.

**Step 2**
Go to System > Security > Phone Security Profile
- Edit the existing configuration, or create a new configuration and associate with the phone
- Check the Enable Digest Authentication box

**Step 3**
Go to User Management > End User
- Create a new user
- Add the User ID, and digest credentials

**Step 4**
Go to the Phone Settings page and associate the user in the Digest User field.

Configure Digest Credentials on Unified E-SRST for SIP

To configure credentials under a specific voice register pool, perform the following procedure:

**SUMMARY STEPS**
1. enable
2. configure terminal
3. voice register pool <pool-tag>
4. username <username> password <password>
5. end
Example: Configuring Digest Credentials on ESRST

The following example shows how to configure digest credentials on ESRST:

Router# conf terminal
Router(config)# voice register pool 10
Router (config-register-pool)# username abc password xyz

Configure Digest Credentials on Unified E-SRST for SCCP

To configure credentials under a specific ephone, perform the following procedure:

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone ephone-tag
4. username username password password
5. end

Unified E-SRST Scale Support

For Unified E-SRST 10.5 to 12.0, the scale of Unified E-SRST mode is increased to match the scale of Classic SRST for both SIP and SCCP Phones.

Table 3-2 lists the scale for number of phones and DNs supported in ESRST mode for Release 10.5 to 12.0.

<table>
<thead>
<tr>
<th>Platform</th>
<th>New Phone Scale</th>
<th>New DN Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2901</td>
<td>35</td>
<td>200</td>
</tr>
<tr>
<td>Cisco 2911</td>
<td>50</td>
<td>300</td>
</tr>
<tr>
<td>Cisco 2921</td>
<td>100</td>
<td>400</td>
</tr>
<tr>
<td>Cisco 2951</td>
<td>250</td>
<td>500</td>
</tr>
<tr>
<td>Cisco 3925</td>
<td>730</td>
<td>1000</td>
</tr>
<tr>
<td>Cisco 3945</td>
<td>1200</td>
<td>1800</td>
</tr>
<tr>
<td>Cisco 3925E</td>
<td>1350</td>
<td>2000</td>
</tr>
<tr>
<td>Cisco 3945E</td>
<td>1500</td>
<td>2500</td>
</tr>
<tr>
<td>Cisco 4451-X</td>
<td>1500</td>
<td>2500</td>
</tr>
<tr>
<td>ISR 4321</td>
<td>35</td>
<td>200</td>
</tr>
<tr>
<td>ISR 4331</td>
<td>100</td>
<td>400</td>
</tr>
<tr>
<td>ISR 4351</td>
<td>730</td>
<td>1000</td>
</tr>
<tr>
<td>ISR 4431</td>
<td>1200</td>
<td>1800</td>
</tr>
<tr>
<td>ISR 4451</td>
<td>1500</td>
<td>2500</td>
</tr>
</tbody>
</table>
Note
The increase in scale mentioned in the table is only for basic calls. For enhanced feature support such as Shared-line, BLF, Video, and VHG, these numbers are not applicable.

Example: ESRST Scale Increase

The following example shows the increase in scale support in the E-SRST mode for ISR 3945E platform:

ESRST_3945e(config-telephony)#max-dn ?
<1-2500> Maximum single/dual/octo line directory numbers supported
ESRST_3945e(config-telephony)#max-ephones ?
<1-1500> Maximum phones to support

Where to Go Next

Proceed to the “Setting Up the Network” section on page 123.
Setting Up the Network

This chapter describes how to configure your Cisco Unified Survivable Remote Site Telephony (SRST) router to run DHCP and to communicate with the IP phones during Cisco Unified Communications Manager fallback.

Contents

- Information About Setting Up the Network, page 124
- How to Set Up the Network, page 124
- Where to Go Next, page 134
Information About Setting Up the Network

When the WAN link fails, the Cisco Unified IP Phones detect that they are no longer receiving keepalive packets from Cisco Unified CM. The Cisco Unified IP Phones then register with the router. The Cisco Unified SRST software is automatically activated and builds a local database of all Cisco Unified IP Phones attached to it (up to its configured maximum). The IP phones are configured to query the router as a backup call-processing source when the central Cisco Unified CM does not acknowledge keepalive packets. The Cisco Unified SRST router now performs call setup and processing, call maintenance, and call termination.

Cisco Unified Communications Manager uses DHCP to provide Cisco Unified IP Phones with the IP address of Cisco Unified Communications Manager. In a remote branch office, DHCP service is typically provided either by the SRST router itself or through the Cisco Unified SRST router using DHCP relay. Configuring DHCP is one of two main tasks in setting up network communication. The other task is configuring the Cisco Unified SRST router to receive messages from the Cisco IP phones through the specified IP addresses. Keepalive intervals are also set at this time.

How to Set Up the Network

This section contains the following tasks:

- **Enabling IP Routing, page 124** (Required)
- **Enabling Cisco Unified SRST on an MGCP Gateway** (Required)
- **Configuring DHCP for Cisco Unified SRST Phones, page 130** (Required)
- **Specifying Keepalive Intervals, page 133** (Optional)

Enabling IP Routing

To initiate SRST service, you need to enable IP routing command and configure an interface that you want to use or bind. For information about enabling IP routing, see *Configuring IP Addressing*.

Enabling Cisco Unified SRST on an MGCP Gateway

To use SRST as your fallback mode with an MGCP gateway, SRST and MGCP fallback must both be configured on the same gateway. The configuration below allows SRST to assume control over the voice port and over call processing on the MGCP gateway. Due to command changes that were made in Cisco IOS Release 12.3(14)T, use the configuration task that corresponds with the Cisco IOS Release you have installed.

The commands described in the configuration below are ineffective unless both commands are configured. For instance, your configuration will not work if you only configure the `ccm-manager fallback-mgcp` command.
When an MGCP-controlled PRI goes into SRST mode, do not make or save configuration changes to the NVRAM on the router. If configuration changes are made and saved in SRST mode, the MGCP-controlled PRI fails when normal MGCP operation is restored.

Configuring Cisco Unified SRST on an MGCP Gateway Prior to Cisco IOS Release 12.3(14)T

Perform this task to enable SRST on a MGCP Gateway if you are using a software release prior to Cisco IOS Release 12.3(14)T.

SUMMARY STEPS

1. enable
2. configure terminal
3. ccm-manager fallback-mgcp
4. call application alternate [application-name]  
   or  
   or  
   service [alternate | default] service-name location
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:</td>
<td>• Enter your password when prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ccm-manager fallback-mgcp</td>
<td>Enables the gateway fallback feature and allows an MGCP voice gateway to provide call processing services through SRST or other configured applications when Cisco Unified Communications Manager is unavailable.</td>
</tr>
</tbody>
</table>
How to Set Up the Network

Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later Releases

Perform this task to enable SRST on an MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later version.

Restrictions

Effective with Cisco IOS Release 12.3(14)T, the call application alternate command is replaced by the service command. The service command can be used in all releases after Cisco IOS Release 12.3(14)T.

Command or Action | Purpose
--- | ---
Step 4 | The call application alternate command specifies that the default voice application takes over if the MGCP application is not available. The application-name argument is optional and indicates the name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.

Step 5 | Exits global configuration mode and returns to privileged EXEC mode.

Example: | Router(config)# exit

Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later Releases

Perform this task to enable SRST on an MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later version.

Restrictions

Effective with Cisco IOS Release 12.3(14)T, the call application alternate command is replaced by the service command. The service command can be used in all releases after Cisco IOS Release 12.3(14)T.

Command or Action | Purpose
--- | ---
Step 4 | The call application alternate command specifies that the default voice application takes over if the MGCP application is not available. The application-name argument is optional and indicates the name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.

Step 5 | Exits global configuration mode and returns to privileged EXEC mode.

Example: | Router(config)# exit

Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later Releases

Perform this task to enable SRST on an MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later version.

Restrictions

Effective with Cisco IOS Release 12.3(14)T, the call application alternate command is replaced by the service command. The service command can be used in all releases after Cisco IOS Release 12.3(14)T.

Command or Action | Purpose
--- | ---
Step 4 | The call application alternate command specifies that the default voice application takes over if the MGCP application is not available. The application-name argument is optional and indicates the name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.

Step 5 | Exits global configuration mode and returns to privileged EXEC mode.

Example: | Router(config)# exit

Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later Releases

Perform this task to enable SRST on an MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later version.

Restrictions

Effective with Cisco IOS Release 12.3(14)T, the call application alternate command is replaced by the service command. The service command can be used in all releases after Cisco IOS Release 12.3(14)T.

Command or Action | Purpose
--- | ---
Step 4 | The call application alternate command specifies that the default voice application takes over if the MGCP application is not available. The application-name argument is optional and indicates the name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.

Step 5 | Exits global configuration mode and returns to privileged EXEC mode.

Example: | Router(config)# exit

Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later Releases

Perform this task to enable SRST on an MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later version.

Restrictions

Effective with Cisco IOS Release 12.3(14)T, the call application alternate command is replaced by the service command. The service command can be used in all releases after Cisco IOS Release 12.3(14)T.

Command or Action | Purpose
--- | ---
Step 4 | The call application alternate command specifies that the default voice application takes over if the MGCP application is not available. The application-name argument is optional and indicates the name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.

Step 5 | Exits global configuration mode and returns to privileged EXEC mode.

Example: | Router(config)# exit
### SUMMARY STEPS

1. enable
2. configure terminal
3. ccm-manager fallback-mgcp
4. application [application-name]
5. global
6. service [alternate | default] service-name location
7. 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: Router&gt; enable</td>
<td>Enter your password when prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ccm-manager fallback-mgcp</td>
<td>Enables the gateway fallback feature and allows an MGCP voice gateway to provide call processing services through SRST or other configured applications when Cisco Unified Communications Manager is unavailable.</td>
</tr>
<tr>
<td>Example: Router(config)# ccm-manager fallback-mgcp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> application [application-name]</td>
<td>The <strong>application-name</strong> argument is optional and indicates the name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.</td>
</tr>
<tr>
<td>Example: Router(config) application app-xfer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> global</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# global</td>
<td></td>
</tr>
</tbody>
</table>
Step 6  
**service [alternate | default] service-name location**

**Example:**

Router(config) service myapp
https://myserver/myfile.vxml

**Step 7**  
**exit**

**Example:**

Router(config)# exit

**Command or Action**  
<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loads and configures a specific, standalone application on a dial peer.</td>
</tr>
<tr>
<td><img src="Optional" alt="alternate" />. Alternate service to use if the service that is configured on the dial peer fails.</td>
</tr>
<tr>
<td><img src="Optional" alt="default" />. Specifies that the default service (“DEFAULT”) on the dial peer is used if the alternate service fails.</td>
</tr>
<tr>
<td>![service-name](Name that identifies the voice application.</td>
</tr>
<tr>
<td>![location](Directory and filename of the Tcl script or VoiceXML document in URL format. For example, flash memory (flash:filename), a TFTP (tftp://../filename), or an HTTP server (http://../filename) are valid locations.</td>
</tr>
</tbody>
</table>

**Configuration Example of Enabling SRST on a MGCP Gateway using Cisco IOS Release 12.3(14)T**

The following is an example of configuring SRST on an MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later release:

```
isdn switch-type primary-net5
!
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager config
mta receive maximum-recipients 0
!
controller E1 1/0
pri-group timeslots 1-12,16 service mgcp
!
controller E1 1/1
!
!
interface Ethernet0/0
ip address 10.48.80.9 255.255.255.0
half-duplex
!
interface Serial1/0:15
no ip address
no logging event link-status
isdn switch-type primary-net5
isdn incoming-voice voice
isdn bind-13 ccm-manager
no cdp enable
!
```
call rsvp-sync
!
call application alternate DEFAULT

!--- For Cisco IOS® Software Release 12.3(14)T or later, this command was replaced by the service command in global application configuration mode.

application
  global
  service alternate Default

!
voice-port 1/0:15
!
mgcp
mgc p dtmf-relay voip codec all mode cisco
mgcp package-capability rtp-package
mgcp sd p simple
!
mgcp profile default
!
!
dial-peer cor custom
!
!

dial-peer voice 10 pots
  application mgcpapp
  incoming called-number
  destination-pattern 9T
  direct-inward-dial
  port 1/0:15

!
!
call-manager-fallback
  limit-dn 7960 2
  ip source-address 10.48.80.9 port 2000
  max-ephones 10
  max-dn 32
  dialplan-pattern 1 704.... extension-length 4
  keepalive 20
  default-destination 5002
  alias 1 5003 to 5002
  call-forward busy 5002
  call-forward noan 5002 timeout 12
  time-format 24

!
!
line con 0
exec-timeout 0 0
line aux
Configuring DHCP for Cisco Unified SRST Phones

To perform this task, you must have your network configured with DHCP. For further details about DHCP configuration, see the Cisco IOS DHCP Server document and see your Cisco Unified Communications Manager documentation.

When a Cisco IP phone is connected to the Cisco Unified SRST system, it automatically queries for a DHCP server. The DHCP server responds by assigning an IP address to the Cisco IP phone and providing the IP address of the TFTP server through DHCP option 150. Then, the phone registers with the Cisco Unified Communications Manager system server and attempts to get configuration and phone firmware files from the Cisco Unified Communications Manager TFTP server address provided by the DHCP server.

When setting up your network, configure your DHCP server local to your site. You may use your SRST router to provide DHCP service (recommended). If your DHCP server is across the WAN and there is an extended WAN outage, the DHCP lease times on your Cisco Unified IP Phones may expire. This may cause your phones to lose their IP addresses, resulting in a loss of service. Rebooting your phones when there is no DHCP server available after the DHCP lease has expired will not reactivate the phones, because they will be unable to obtain an IP address or other configuration information. Having your DHCP server local to your remote site ensures that the phones can continue to renew their IP address leases in the event of an extended WAN failure.

Choose one of the following tasks to set up DHCP service for your Cisco Unified IP Phones:

- **Defining a Single DHCP IP Address Pool, page 130**: Use this method if the Cisco Unified SRST router is a DHCP server and if you can use a single shared address pool for all your DHCP clients.
- **Defining a Separate DHCP IP Address Pool for Each Cisco Unified IP Phone, page 131**: Use this method if the Cisco Unified SRST router is a DHCP server and you need separate pools for non-IP-phone DHCP clients.
- **Defining the DHCP Relay Server, page 132**: Use this method if the Cisco Unified SRST router is not a DHCP server and you want to relay DHCP requests from IP phones to a DHCP server on a different router.

### Defining a Single DHCP IP Address Pool

This task creates a large shared pool of IP addresses in which all DHCP clients receive the same information, including the option 150 TFTP server IP address. The benefit of selecting this method is that you set up only one DHCP pool. However, defining a single DHCP IP address pool can be a problem if non-IP phone clients need to use a different TFTP server address.

**SUMMARY STEPS**

1. `ip dhcp pool pool-name`
2. `network ip-address [mask | prefix-length]`
3. `option 150 ip ip-address`
4. `default-router ip-address`
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></td>
</tr>
<tr>
<td><code>ip dhcp pool pool-name</code></td>
<td>Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip dhcp pool mypool</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`network ip-address [mask</td>
<td>Specifies the IP address of the DHCP address pool and the optional mask or number of bits in the address prefix, preceded by a forward slash.</td>
</tr>
<tr>
<td></td>
<td>prefix-length]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcp)# network 10.0.0.0 255.255.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>option 150 ip ip-address</code></td>
<td>Specifies the TFTP server address from which the Cisco IP phone downloads the image configuration file. This needs to be the IP address of Cisco Unified CM.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcp)# option 150 ip 10.0.22.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>default-router ip-address</code></td>
<td>Specifies the router to which the Cisco Unified IP phones are connected directly.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcp)# default-router 10.0.0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits DHCP pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dhcp)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Defining a Separate DHCP IP Address Pool for Each Cisco Unified IP Phone

This task creates a name for the DHCP server address pool and specifies IP addresses. This method requires you to make an entry for every Cisco Unified IP phone.

### SUMMARY STEPS

1. `ip dhcp pool pool-name`
2. `host ip-address subnet-mask`
3. `option 150 ip ip-address`
4. `default-router ip-address`
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>ip dhcp pool pool-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# ip dhcp pool pool2</td>
</tr>
<tr>
<td>Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | host ip-address subnet-mask |
| **Example:** | Router(config-dhcp)# host 10.0.0.0 255.255.0.0 |
| Specifies the IP address that you want the phone to use. |

| **Step 3** | option 150 ip ip-address |
| **Example:** | Router(config-dhcp)# option 150 ip 10.0.22.1 |
| Specifies the TFTP server address from which the Cisco IP phone downloads the image configuration file. This needs to be the IP address of Cisco Unified CM. |

| **Step 4** | default-router ip-address |
| **Example:** | Router(config-dhcp)# default-router 10.0.0.1 |
| Specifies the router to which the Cisco Unified IP phones are connected directly. |
| • This router should be the Cisco Unified SRST router because this is the default address that is used to obtain SRST service in the event of a WAN outage. As long as the Cisco IP phones have a connection to the Cisco Unified SRST router, the phones are able to get the required network details. |

| **Step 5** | exit |
| **Example:** | Router(config-dhcp)# exit |
| Exits DHCP pool configuration mode. |

Defining the DHCP Relay Server

This task sets up DHCP relay on the LAN interface where the Cisco Unified IP phones are connected and enables the Cisco IOS DHCP server feature to relay requests from DHCP clients (phones) to a DHCP server. For further details about DHCP configuration, see the Cisco IOS DHCP Server document.

The Cisco IOS DHCP server feature is enabled on routers by default. If the DHCP server is not enabled on your Cisco Unified SRST router, use the following steps to enable it.

SUMMARY STEPS

1. service dhcp
2. interface type number
3. ip helper-address ip-address
4. exit
Chapter 4  Setting Up the Network

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>service dhcp</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# service dhcp</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface type number</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface serial 0</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip helper-address ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# ip helper-address 10.0.22.1</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# exit</td>
</tr>
</tbody>
</table>

Specifying Keepalive Intervals

The keepalive interval is the period of time between keepalive messages sent by a network device. A keepalive message is a message sent by one network device to inform another network device that the virtual circuit between the two is still active.

Note: If you plan to use the default time interval between messages, which is 30 seconds, you do not have to perform this task.

SUMMARY STEPS

1. call-manager-fallback
2. keepalive seconds
3. exit
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> keepalive seconds</td>
<td>Sets the time interval, in seconds, between keepalive messages that are sent to the router by Cisco Unified IP Phones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# keepalive 60</td>
<td></td>
</tr>
<tr>
<td>• seconds: Range is 10 to 65535. Default is 30.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example sets a keepalive interval of 45 seconds:

```
call-manager-fallback
keepalive 45
```

**Where to Go Next**

The next step is setting up the phone and getting a dial tone. For instructions, see the “Cisco Unified SIP SRST 4.1” section on page 135.

For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
Cisco Unified SIP SRST 4.1

This chapter describes the features and provides the configuration information for Cisco Unified SIP SRST 4.1:

- Out-of-Dialog REFER(OOD-R)
- Digit Collection on SIP Phones
- Caller ID Display
- Disabling SIP Supplementary Services for Call Forward and Call Transfer
- Idle Prompt Status

Note

With Cisco IOS Release 12.4(15)T, the number of SIP phones supported on each platform is now equivalent to the number of SCCP phones supported. For example, 3845 now supports 720 phones regardless of whether these are SIP or SCCP.

Contents

- Prerequisites for Cisco Unified SIP SRST 4.1, page 135
- Restrictions for Cisco Unified SIP SRST 4.1, page 136
- Information About Cisco Unified SIP SRST 4.1, page 136
- How to Configure Cisco Unified SIP SRST 4.1 Features, page 139
- Where to Go Next, page 143

Prerequisites for Cisco Unified SIP SRST 4.1

- Cisco IOS Release 12.4(15)T or a later release.
- Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE require firmware load 8.2(1) or a later version.
- For the prerequisites for the Enhanced 911 Services for Cisco Unified SRST feature introduced in Version 4.1, see Prerequisites for Enhanced 911 Services.
Restrictions for Cisco Unified SIP SRST 4.1

- Cisco Unified SRST does not support BLF speed-dial notification, call forward all synchronization, dial plans, directory services, or music-on-hold (MOH).
- Prior to SIP phone load 8.0, SIP phones maintained dual registration with both Cisco Unified Communications Manager and Cisco Unified SRST simultaneously. In SIP phone load 8.0 and later versions, SIP phones use keepalive to maintain a connection with Cisco Unified SRST during active registration with Cisco Unified Communications Manager. Every 2 minutes, a SIP phone sends a keepalive message to Cisco Unified SRST. Cisco Unified SRST responds to this keepalive with a 404 message. This process repeats until fallback to Cisco Unified SRST occurs. After fallback, SIP phones send a keepalive message every two minutes to Cisco Unified Communications Manager while the phones are registered with Cisco Unified SRST. Cisco Unified SRST continues to support dual registration for SIP phone loads older than 8.0.

Information About Cisco Unified SIP SRST 4.1

- Out-of-Dialog REFER, page 136
- Digit Collection on SIP Phones, page 137
- Caller ID Display, page 138
- Disabling SIP Supplementary Services for Call Forward and Call Transfer, page 138
- Idle Prompt Status, page 138
- Enhanced 911 Services, page 138

Out-of-Dialog REFER

Out-of-dialog REFER (OOD-R) enables remote applications to establish calls by sending a REFER message to Cisco Unified SRST without an initial INVITE. After the REFER is sent, the remainder of the call setup is independent of the application and the media stream does not flow through the application. The application using OOD-R triggers a call setup request that specifies the Referee address in the Request-URI and the Refer-Target in the Refer-To header. The SIP messaging used to communicate with Cisco Unified SRST is independent of the end-user device protocol, which can be H.323, plain old telephone service (POTS), SCCP, or SIP. Click-to-dial is an example of an application that can be created using OOD-R.

A click-to-dial application enables users to combine multiple steps into one click for a call setup. For example, a user can click a web-based directory application from his or her PC to look up a telephone number, off-hook the desktop phone, and dial the called number. The application initiates the call setup without the user having to out-dial from his or her own phone. The directory application sends a REFER message to Cisco Unified SRST, which sets up the call between both parties based on this REFER.

For more information about OOD-R, see Out-of-Dialog REFER from the Cisco Unified Communications Manager Express System Administrator Guide.
Digit Collection on SIP Phones

Digit strings dialed by phone users must be collected and matched against predefined patterns to place calls to the destination corresponding to the user's input. Previously, SIP phones in a Cisco Unified SRST system required users to press the DIAL soft key or # key, or wait for the interdigit-timeout to trigger call processing. This could cause delays in processing the call.

Two new methods of collecting and matching digits are supported for SIP phones depending on the model of the phone:

- KPML Digit Collection, page 137
- SIP Dial Plans, page 137

KPML Digit Collection

The Key Press Markup Language (KPML) uses SIP SUBSCRIBE and NOTIFY methods to report user input digit by digit. Each digit dialed by the phone user generates its own signaling message to Cisco Unified SRST, which performs pattern recognition by matching a destination pattern to a dial peer as it collects the dialed digits. This process of relaying each digit immediately is similar to the process used by SCCP phones. It eliminates the need for the user to press the Dial soft key or wait for the interdigit timeout before the digits are sent to the Cisco Unified SRST for processing.

KPML is supported on Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE. For configuration information, see the “Enabling KPML for SIP Phones” section on page 139.

SIP Dial Plans

A dial plan is a set of dial patterns that SIP phones use to determine when digit collection is complete after a user goes off-hook and dials a destination number. Dial plans enable SIP phones to perform local digit collection and recognize dial patterns as user input is collected. After a pattern is recognized, the SIP phone sends an INVITE message to Cisco Unified SRST to initiate the call to the number matching the user's input. All of the digits entered by the user are presented as a block to Cisco Unified SRST for processing. Because digit collection is done by the phone, dial plans reduce signaling messages overhead compared to KPML digit collection.

SIP dial plans eliminate the need for a user to press the Dial soft key or # key or to wait for the interdigit timeout to trigger an outgoing INVITE. You configure a SIP dial plan and associate the dial plan with a SIP phone. The dial plan is downloaded to the phone in the configuration file.

You can configure SIP dial plans and associate them with the following SIP phones:

- Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE: These phones use dial plans and support KPML. If both a dial plan and KPML are enabled, the dial plan has priority.
  
  If a matching dial plan is not found and KPML is disabled, the user must wait for the interdigit timeout before the SIP NOTIFY message is sent to Cisco Unified SRST. Unlike other SIP phones, these phones do not have a Dial soft key to indicate the end of dialing, except when on-hook dialing is used.

- Cisco Unified IP Phone 7905, 7912, 7940, and 7960: These phones use dial plans and do not support KPML. If you do not configure a SIP dial plan for these phones, or if the dialed digits do not match a dial plan, the user must press the Dial soft key or wait for the interdigit timeout before digits are sent to Cisco Unified SRST for processing.
When you reset a phone, the phone requests its configuration files from the TFTP server, which builds the appropriate configuration files depending on the type of phone.

- Cisco Unified IP Phone 7905 and 7912: The dial plan is a field in their configuration files.
- Cisco Unified IP Phone 7911G, 7940, 7941G, 7941GE, 7960, 7961G, 7961GE, 7970G, and 7971GE: The dial plan is a separate XML file that is pointed to from the normal configuration file.

The Cisco Unified SRST supports SIP dial plans if they are provisioned in Cisco Unified Communications Manager. You cannot configure dial plans in Cisco Unified SRST.

**Caller ID Display**

The name and number of the caller is included in the Caller ID display on the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE. Other SIP phones display only the number of the caller. Also, the caller ID information is updated on the destination phone when there is a change in the caller ID of the originating party such as with call forwarding or call transfer. No new configuration is required to support these enhancements.

**Disabling SIP Supplementary Services for Call Forward and Call Transfer**

If a destination gateway does not support supplementary services, you can disable REFER messages for call transfers and redirect responses for call forwarding from being sent by Cisco Unified SRST.

Disabling supplementary services is supported if all endpoints use SCCP or all endpoints use SIP. It is not supported for a mix of SCCP and SIP endpoints.

**Idle Prompt Status**

A message displays on the status line of a SIP phone after the phone registers to Cisco Unified SRST to indicate that Cisco Unified SRST is providing fallback support for the Cisco Unified Communications Manager. This message informs the user that the phone is operating in fallback mode and that not all features are available. The default message that displays “CM Fallback Service Operating” is taken from the phone dictionary file. You can customize the message by using the system message command on the Cisco Unified SRST router. Cisco Unified SRST updates the idle prompt message when a SIP phone registers or when you modify the message through the configuration. The message displays until a phone switches back to the Cisco Unified Communications Manager.

The idle prompt status message is supported for the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE with Cisco Unified SRST 4.1 and later versions. For versions earlier than Cisco Unified SRST 4.1, the phones display the default message from the dictionary file.

**Enhanced 911 Services**

Enhanced 911 Services for Cisco Unified SRST enables 911 operators to:

- Immediately pinpoint the location of the 911 caller based on the calling number
- Callback the 911 caller if a disconnect occurs

Before this feature was introduced, Cisco Unified SRST supported only outbound calls to 911. With basic 911 functionality, calls were simply routed to a Public Safety Answering Point (PSAP). The 911 operator at the PSAP would then have to verbally gather the emergency information and location from
the caller, before dispatching a response team from the ambulance service, fire department, or police department. Calls could not be routed to different PSAPs, based on the specific geographic areas that they cover.

With Enhanced 911 Services, 911 calls are selectively routed to the closest PSAP based on the caller’s location. In addition, the caller’s phone number and address automatically display on a terminal at the PSAP. Therefore, the PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

See Configuring Enhanced 911 Services from Cisco Unified Communications Manager Express System Administrator Guide for more information.

How to Configure Cisco Unified SIP SRST 4.1 Features

This section contains the following tasks:

- Enabling KPML for SIP Phones, page 139
- Disabling SIP Supplementary Services for Call Forward and Call Transfer, page 141
- Configuring Idle Prompt Status for SIP Phones, page 142

Enabling KPML for SIP Phones

Perform the following steps to enable KPML digit collection on a SIP phone.

Restrictions

- This feature is supported only on Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.
- A dial plan assigned to a phone has priority over KPML.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool pool-tag
4. digit collect kpml
5. end
6. show voice register dial-peer
## 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>Router&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></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register pool pool-tag</td>
<td>Enter voice register pool configuration mode to set phone-specific parameters for a SIP phone.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice register pool 4</td>
<td>• pool-tag: Unique sequence number of the SIP phone to be configured. Range is version and platform-dependent; type ? to display range. You can modify the upper limit for this argument with the max-pool command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> digit collect kpml</td>
<td>Enables KPML digit collection for the SIP phone.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Note This command is enabled by default for supported phones in Cisco Unified CME and Cisco Unified SRST.</td>
</tr>
<tr>
<td>Router(config-register-pool)# digit collect kpml</td>
<td>Exit privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-register-pool)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show voice register dial-peers</td>
<td>Displays details of all dynamically created VoIP dial peers associated with the Cisco Unified CME SIP register including the defined digit collection method.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show voice register dial-peers</td>
<td></td>
</tr>
</tbody>
</table>

### What to Do Next

After changing the KPML configuration in Cisco Unified SRST, you do not need to create new configuration profiles and restart the phones. Enabling or disabling KPML is effective immediately in Cisco Unified SRST.
Disabling SIP Supplementary Services for Call Forward and Call Transfer

Perform the following steps to disable REFER messages for call transfers and redirect responses for call forwarding from being sent to the destination by Cisco Unified SRST. You can disable these supplementary features if the destination gateway does not support them.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
   or
   dial-peer voice tag voip
4. no supplementary-service sip {moved-temporarily | refer}
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: Router&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: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode to set global parameters for VoIP features.</td>
</tr>
<tr>
<td>or</td>
<td>or</td>
</tr>
<tr>
<td>dial-peer voice tag voip</td>
<td>Enters dial peer configuration mode to set parameters for a specific dial peer.</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 99 voip</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Idle Prompt Status for SIP Phones

Perform the following steps to customize the message that displays on SIP phones after the phones failover to Cisco Unified SRST.

**Note** You do not need to create new configuration files with the `create profile` command and restart the phones after changing the idle status message in Cisco Unified SRST. Modifying the status message takes effect immediately in Cisco Unified SRST.

**Prerequisites**

Cisco Unified SRST 4.1 or a later version.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice register global
4. system message `string`
5. end
6. show voice register global

---

**Command or Action**

**Step 4**

`no supplementary-service sip {moved-temporarily refer}`

**Example:**

Router(conf-voi-serv)# no supplementary-service sip refer
or
Router(config-dial-peer)# no supplementary-service sip refer

**Step 5**

`end`

**Example:**

Router(config-voi-serv)# end
or
Router(config-dial-peer)# end

**Purpose**

Disables SIP call forwarding or call transfer supplementary services globally or for a dial peer.

- **moved-temporarily**: SIP redirect response for call forwarding.
- **refer**: SIP REFER message for call transfers.
- Sending REFER and redirect messages to the destination is the default behavior.

**Note** This command is supported for calls between SIP phones and calls between SCCP phones. It is not supported for a mixture of SCCP and SIP endpoints.

Exits to privileged EXEC mode.
The next step is configuring Cisco Unified IP phones using SCCP. For instructions, see the “Setting Up Cisco Unified IP Phones using SCCP” section on page 145.

For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
CHAPTER 6

Setting Up Cisco Unified IP Phones using SCCP

This chapter describes how to set up the displays and features that callers will see and use on Cisco Unified IP Phones during Cisco Unified CM fallback.

Note
Cisco Unified IP Phones discussed in this chapter are just examples. For a complete list of IP phones, see Compatibility Information.

Contents

- Information About Setting Up Cisco Unified IP Phones, page 145
- How to Set Up Cisco Unified IP Phones, page 146
- How to Set Up Cisco IP Communicator for Cisco Unified SRST, page 162
- Where to Go Next, page 163

Information About Setting Up Cisco Unified IP Phones

Cisco Unified IP Phone configuration is limited for Cisco Unified SRST because IP phones retain nearly all Cisco Unified CM settings during Cisco Unified CM fallback. You can configure the date format, time format, language, and system messages that appear on Cisco Unified IP Phones during Cisco Unified Communications Manager fallback. All four of these settings have defaults, and the available language options depend on the IP phones and Cisco Unified CM version in use. Also available for configuration is a secondary dial tone, which can be generated when a phone user dials a predefined PSTN access prefix and can be terminated when additional digits are dialed. Dual-line phone configuration is required for dual-line phone operation during Cisco Unified CM fallback.
How to Set Up Cisco Unified IP Phones

This section contains the following tasks:

- Configuring Cisco Unified SRST to Support Phone Functions, page 146 (Required)
- Configuring Cisco Unified 8941 and 8945 SCCP IP Phones, page 148 (Required)
- Verifying That Cisco Unified SRST Is Enabled, page 149 (Optional)
- Configuring IP Phone Clock, Date, and Time Formats, page 150 (Optional)
- Configuring IP Phone Language Display, page 152 (Optional)
- Configuring Customized System Messages for Cisco Unified IP Phones, page 154 (Optional)
- Configuring a Secondary Dial Tone, page 155 (Optional)
- Configuring Dual-Line Phones, page 156 (Required Under Certain Conditions)
- Configuring Eight Calls per Button (Octo-Line), page 158 (Optional)
- Configuring the Maximum Number of Calls, page 160 (Optional)
- Troubleshooting, page 162 (Optional)

Configuring Cisco Unified SRST to Support Phone Functions

Tip

When the Cisco Unified SRST is enabled, Cisco Unified IP Phones do not have to be reconfigured while in Cisco Unified Communications Manager fallback mode because phones retain the same configuration that was used with Cisco Unified Communications Manager.

To configure Cisco Unified SRST on the router to support the Cisco Unified IP Phone functions, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. `call-manager-fallback`
2. `ip source-address ip-address [port port] [any-match | strict-match]`
3. `max-dn max-directory-numbers [dual-line] [preference preference-order]`
4. `max-ephones max-phones`
5. `limit-dn phone-type max-lines`
6. `exit`
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip source-address ip-address [port port] [any-match</td>
<td>strict-match]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# ip source-address 10.6.21.4 port 2002 strict-match</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> max-dn max-directory-numbers [dual-line] [preference preference-order]</td>
<td>Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router and activates the dual-line mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-dn 15 dual-line preference 1</td>
<td>• <em>max-directory-numbers:</em> Maximum number of directory numbers (dns) or virtual voice ports supported by the router. The maximum number is platform-dependent. The default is 0. See <em>Compatibility Information</em> for further details.</td>
</tr>
<tr>
<td></td>
<td>• <em>preference preference-order</em> (Optional). Sets the global preference for creating the VoIP dial peers for all directory numbers that are associated with the primary number. Range is from 0 to 10. Default is 0, which is the highest preference. The <em>alias</em> command also has a <em>preference</em> keyword that sets <em>alias</em> command preference values. Setting the <em>alias</em> command <em>preference</em> keyword allows the default preference set with the <em>max-dn</em> command to be overridden. See the “Configuring Call Rerouting” section on page 190 for more information on using the <em>max-dn</em> command with the <em>alias</em> command.</td>
</tr>
<tr>
<td><strong>Note</strong> You must reboot the router to reduce the limit of the directory numbers or virtual voice ports after the maximum allowable number is configured.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> max-ephones max-phones</td>
<td>Configures the maximum number of Cisco IP phones that can be supported by the router. The default is 0. The maximum number is platform dependent. See <em>Compatibility Information</em> for further details.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-ephones 24</td>
<td><strong>Note</strong> You must reboot the router to reduce the limit of Cisco IP phones after the maximum allowable number is configured.</td>
</tr>
</tbody>
</table>
### Configuring Cisco Unified 8941 and 8945 SCCP IP Phones

To configure Cisco Unified 8941 and 8945 SCCP IP Phones in SRST mode, perform the following commands:

**Note** This section is required only in SRST version 8.6 and is not required for version 8.6 and higher.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ephone-type phone-type`
4. `device-id number`
5. `device-type phone-type`
6. `end`

---

**Command or Action** | **Purpose**
--- | ---
**Step 5** | `limit-dn phone-type max-lines` (Optional) Limits the directory number lines on Cisco IP phones during Cisco Unified CM fallback.
**Example:**
Router(config-cm-fallback)# limit-dn 7945 2
**Note** You must configure this command during initial Cisco Unified SRST router configuration, before any phone actually registers with the Cisco Unified SRST router. However, you can modify the number of lines at a later time.

For a list of available phones, see *Cisco SRST and SIP SRST Command Reference (All Versions)*.

The setting for maximum lines is from 1 to 6. The default number of maximum directory lines is set to 6. If there is any active phone with the last line number greater than this limit, warning information is displayed for phone reset.

**Step 6** | `exit` Exits call-manager-fallback configuration mode.
**Example:**
Router(config-cm-fallback)# 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:</td>
<td>Enters 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>Step 3 ephone-type phone-type</td>
<td>Enters phone type to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td>8941</td>
</tr>
<tr>
<td></td>
<td>8945</td>
</tr>
<tr>
<td>Step 4 device-id number</td>
<td>Specifies the device ID for the phone type.</td>
</tr>
<tr>
<td>Example:</td>
<td>8941—586</td>
</tr>
<tr>
<td></td>
<td>8945—585</td>
</tr>
<tr>
<td>Step 5 device-type phone-type</td>
<td>Specifies the device type for the phone.</td>
</tr>
<tr>
<td>Example:</td>
<td>8941</td>
</tr>
<tr>
<td></td>
<td>8945</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Verifying That Cisco Unified SRST Is Enabled

To verify that the Cisco Unified SRST feature is enabled, perform the following steps:

Step 1 Enter the `show running-config` command to verify the configuration.

Step 2 Enter the `show call-manager-fallback all` command to verify that the Cisco Unified SRST feature is enabled.

Step 3 Use the Settings display on the Cisco IP phones in your network to verify that the default router IP address on the phones matches the IP address of the Cisco Unified SRST router.
**Step 4**

To temporarily block the TCP port 2000 Skinny Client Control Protocol (SCCP) connection for one of the Cisco IP phones to force the Cisco IP phone to lose its connection to the Cisco Unified Communications Manager and register with the Cisco Unified SRST router, perform the following steps:

a. Use the appropriate IP `access-list` command to temporarily disconnect a Cisco Unified IP Phone from the Cisco Unified Communications Manager.

During a WAN connection failure, when Cisco Unified SRST is enabled, Cisco Unified IP Phones display a message informing you that they are operating in Cisco Unified Communications Manager fallback mode. The Cisco IP Phone 7960 and Cisco IP Phone 7940 display a “CM Fallback Service Operating” message, and the Cisco IP Phone 7910 displays a “CM Fallback Service” message when operating in Cisco Unified Communications Manager fallback mode. When the Cisco Unified Communications Manager is restored, the message goes away and full Cisco IP phone functionality is restored.

b. Use the `debug ephone register` command to observe the registration process of the Cisco IP phone on the Cisco Unified SRST router.

c. Use the `show ephone` command to display the Cisco IP phones that have registered to the Cisco Unified SRST router.

d. Enter the `no` form of the appropriate `access-list` command to restore normal service for the phone.

---

**Configuring IP Phone Clock, Date, and Time Formats**

The Cisco Unified IP Phone 7970G and Cisco Unified IP Phone 7971G-GE IP phones obtain the correct timezone from Cisco Unified Communications Manager. They also receive the Coordinated Universal Time (UTC) time from the SRST router during SRST registration. When in SRST mode, the phones take the timezone and the UTC time, and apply a timezone offset to produce the correct time display.

Cisco IP Phone 7960 IP phones and other similar SCCP phones such as the Cisco IP Phone 7940, get their display clock information from the local time of the SRST router during SRST registration. If the Cisco Unified SRST router is configured to use the Network Time Protocol (NTP) to automatically sync the Cisco Unified SRST router time from an NTP time server, only UTC time is delivered to the router. This is because the NTP server could be physically located anywhere in the world, in any timezone. As it is important to display the correct local time, use the `clock timezone` command to adjust or offset the Cisco Unified SRST router time.

The date and time formats that appear on the displays of all Cisco Unified IP Phones in Cisco Unified CM fallback mode are selected using the `date-format` and `time-format` commands as configured below:

**SUMMARY STEPS**

1. `clock timezone zone hours-offset [minutes-offset]`
2. `call-manager-fallback`
3. `date-format { mm-dd-yy | dd-mm-yy | yy-dd-mm | yy-mm-dd }`
4. `time-format { 12 | 24 }`
5. `exit`
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> clock timezone <strong>zone</strong> hours-offset [minutes-offset]</td>
<td>Sets the time zone for display purposes.</td>
</tr>
</tbody>
</table>
| **Example:** Router(config)# clock timezone PST -8 | - **zone**: Name of the time zone to be displayed when standard time is in effect. The length of the zone argument is limited to 7 characters.  
- **hours-offset**: The number of hour difference from Coordinated Universal Time (UTC).  
- **minutes-offset** (Optional). Minutes difference from UTC. |
| **Step 2** call-manager-fallback | Enters call-manager-fallback configuration mode. |
| **Example:** Router(config)# call-manager-fallback | |
| **Step 3** date-format {mm-dd-yy | dd-mm-yy | yy-dd-mm | yy-mm-dd} | Sets the date format for IP phone display. The choices are mm-dd-yy, dd-mm-yy, yy-dd-mm, and yy-mm-dd, where  
- **dd**: day  
- **mm**: month  
- **yy**: year  
The default is set to mm-dd-yy. |
| **Example:** Router(config-cm-fallback)# date-format yy-dd-mm | |
| **Step 4** time-format {12 | 24} | Sets the time display format on all Cisco Unified IP Phones registered with the router. The default is set to a 12-hour clock. |
| **Example:** Router(config-cm-fallback)# time-format 24 | |
| **Step 5** exit | Exits call-manager-fallback configuration mode. |
| **Example:** Router(config-cm-fallback)# exit | |

### Example

The following example sets the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC and sets the time display format to a 24 hour clock:

Router(config)# clock timezone PST -8
Router(config)# call-manager-fallback
Router(config-cm-fallback)# time-format 24
Configuring IP Phone Language Display

During Cisco Unified CM fallback, the language displays shown on Cisco Unified IP Phones default to the ISO-3166 country code of US (United States). The Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7960 can be configured for different languages (character sets and spelling conventions) using the user-locale command.

Note
This configuration option is available in Cisco SRST V2.1 and later versions running under Cisco Unified CM V3.2 and later versions. Systems with software prior to Cisco Unified SRST V2.1 and Cisco Unified CM V3.2 can use the default country, United States (US), only.

SUMMARY STEPS

1. call-manager-fallback
2. user-locale country-code
3. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> user-locale country-code</td>
<td>Selects a language by country for displays on the Cisco IP Phone 7940 and Cisco IP Phone 7960.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# user-locale ES</td>
<td>Selects a language by country for displays on the Cisco IP Phone 7940 and Cisco IP Phone 7960.</td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td>Exits configuration mode.</td>
</tr>
</tbody>
</table>

### Examples

The following example offers a configuration for the Portugal user locale:

```
call-manager-fallback
user-locale PT
```
Configuring Customized System Messages for Cisco Unified IP Phones

Use the system message command to customize the system message displayed on all Cisco Unified IP Phones during Cisco Unified CM fallback.

One of two keywords, primary and secondary, must be included in the command. The primary keyword is for IP phones that can support static text messages during fallback. The default display message for primary IP phones in fallback mode is “CM Fallback Service Operating.”

The secondary keyword is for Cisco Unified IP Phones that do not support static text messages and have a limited display space. Secondary IP phones flash messages during fallback. The default display message for secondary IP phones in fallback mode is “CM Fallback Service.”

Changes to the display message will occur immediately after configuration or at the end of each call.

**Note**

The normal in-service static text message is controlled by Cisco Unified Communications Manager.

**SUMMARY STEPS**

1. call-manager-fallback
2. system message {primary primary-string | secondary secondary-string}
3. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td>Step 2 system message {primary primary-string</td>
<td>secondary secondary-string}</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# system message primary Custom Message</td>
<td></td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Examples

The following example sets “SRST V3.0” as the system display message for all Cisco Unified IP Phones on a router:

```
call-manager-fallback
system message primary SRST V3.0
system message secondary SRST V3.0
exit
```

Configuring a Secondary Dial Tone

A secondary dial tone can be generated when a phone user dials a predefined PSTN access prefix and can be terminated when additional digits are dialed. An example is when a secondary dial tone is heard after the number 9 is dialed to reach an outside line.

**SUMMARY STEPS**

1. call-manager-fallback
2. secondary-dialtone digit-string
3. 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>call-manager-fallback</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# call-manager-fallback</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>secondary-dialtone digit-string</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-cm-fallback)# secondary-dialtone digit-string</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-cm-fallback)# exit</td>
</tr>
</tbody>
</table>

**Examples**

The following example sets the number 8 to trigger a secondary dial tone:

```
call-manager-fallback
secondary-dialtone 8
```
Configuring Dual-Line Phones

Dual-line phone configuration is required for dual-line phone operation during Cisco Unified CM fallback, see the “Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0” section on page 208.

Dual-line IP phones are supported during Cisco Unified CM fallback using the \texttt{max-dn} command. Dual-line IP phones have one voice port with two channels to handle two independent calls. This capability enables call waiting, call transfer, and conference functions on a phone-line button.

In dual-line mode, each IP phone and its associated line button can support one or two calls. Selection of one of two calls on the same line is made using the blue Navigation button located below the phone display. When one of the dual-line channels is used on a specific phone, other phones that share the ephone-dn will be unable to use the secondary channel. The secondary channel will be reserved for use with the primary dual-line channel.

It is recommended that hunting be disabled to the second channel. For more information, see the “Configuring Dial-Peer and Channel Hunting” section on page 204.

SUMMARY STEPS

1. call-manager-fallback
2. \texttt{max-dn} \texttt{max-directory-numbers [dual-line] [preference preference-order]}
3. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> max-dn max-directory-numbers [dual-line]</td>
<td>Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router and activates dual-line mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# max-dn 15 dual-line</td>
<td></td>
</tr>
<tr>
<td>preference 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example sets the maximum number of DNs or virtual voice ports that can be supported by a router to 10 and activates the dual-line mode for all IP phones in Cisco Unified CM fallback mode:

```
call-manager-fallback
max-dn 10 dual-line
exit
```
Configuring Eight Calls per Button (Octo-Line)

The octo-line feature supports up to eight active calls, both incoming and outgoing, on a single button. Eight incoming calls to an octo-line directory number ring simultaneously. After an incoming call is answered, the ringing stops and the remaining seven incoming calls hear a call waiting tone.

After an incoming call on an octo-line directory number is answered, the answering phone is in the connected state. Other phones that share the directory number are in the remoteMultiline state. A subsequent incoming call sends the call waiting tone to the phone connected to the call, and sends the ringing tone to the other phones that are in the remoteMultiline state. All phones sharing the directory number can pick up any of the incoming unanswered calls.

When multiple incoming calls ring on an octo-line directory number that is shared among multiple phones, the ringing tone stops on the phone that answers the call, and the call waiting tone is heard for other unanswered calls. The multiple instances of the ringing calls is displayed on other ephones sharing the directory number. After a connected call on an octo-line directory number is put on-hold, any phone that shares this directory number can pick up the held call. If a phone is in the process of transferring a call or creating a conference, other phones that share the octo-line directory number cannot steal the call.

As new calls come in on an octo-line, the system searches for the next available idle line using the `huntstop chan tag` command, where `tag` is a number from 1 to 8. An idle channel is selected from the lowest number to the highest. When the highest number of allowed calls is received, the system stops hunting for available channels. Use this command to limit the number of incoming calls on an octo-line directory number and reserve channels for outgoing calls or features such as call transfer or conference calls.

With the new feature, you can:

- Configure only dual-line mode
- Configure only octo-line mode
- Configure dual-line mode and octo-line mode

Prerequisites

- Cisco Unified SRST 7.0/4.3
- Cisco Unified CM 6.0
- Cisco IOS Release 12.4(15)XZ

Restrictions

Octo-line directory numbers are not supported by the Cisco Unified IP Phone 7902, 7920, or 7931, or by analog phones connected to Cisco ATA or Cisco VG224.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `max-dn max-no-of-directories [dual-line | octo-line] [number octo-line]`
5. `huntstop channel 1-8`
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></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Router&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></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> max-dn max-no-of-directories [dual-line</td>
<td>Sets the maximum number of DNs or virtual voice ports</td>
</tr>
<tr>
<td>octo-line] [number octo-line]</td>
<td>that can be supported by the router and activates dual-line</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>mode, octo-line mode, or both modes.</td>
</tr>
<tr>
<td>Router(config-cm-fallback)# max-dn 15 dual-line 6 octo-line</td>
<td>• <strong>max-no-of-directories</strong>: Maximum number of directory</td>
</tr>
<tr>
<td></td>
<td>numbers (dns) or virtual voice ports supported by the</td>
</tr>
<tr>
<td></td>
<td>router. The maximum number is platform-dependent. The</td>
</tr>
<tr>
<td></td>
<td>default is 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dual-line</strong>: (Optional) Allows IP phones in</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager fallback</td>
</tr>
<tr>
<td></td>
<td>mode to have a virtual voice port with two channels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>octo-line</strong>: (Optional) Allows IP phones in</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager fallback</td>
</tr>
<tr>
<td></td>
<td>mode to have a virtual voice port with eight channels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>number</strong> (Optional): Sets the number of directory</td>
</tr>
<tr>
<td></td>
<td>numbers for octo-mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> huntstop channel 1-8</td>
<td>Enables channel huntstop on an octo-line, which keeps a</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>call from hunting to the next channel of a directory number</td>
</tr>
<tr>
<td>Router(config-cm-fallback)# huntstop channel 4</td>
<td>if the last allowed channel is busy or does not answer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>number</strong>: Number of channels available to accept</td>
</tr>
<tr>
<td></td>
<td>incoming calls. The remaining channels are reserved for</td>
</tr>
<tr>
<td></td>
<td>outgoing calls and features such as call transfer,</td>
</tr>
<tr>
<td></td>
<td>call waiting, and conferencing. The range is 1 to 8 and</td>
</tr>
<tr>
<td></td>
<td>the default is 8.</td>
</tr>
<tr>
<td></td>
<td>• The command is supported for octo-line directory</td>
</tr>
<tr>
<td></td>
<td>numbers only.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Examples

In the following example, octo-line mode is enabled, there are 8 octo-line directory numbers, there are a maximum of 23 directory numbers, and a maximum of 6 channels are available for incoming calls:

```
call-manager-fallback
max-dn 23 octo-line 8
huntstop channel 6
```

Configuring the Maximum Number of Calls

To configure the maximum number of calls on a Cisco Unified SCCP IP phone in Cisco Unified SRST 9.0, perform the following steps.

Prerequisites

- Cisco Unified SRST 9.0 and later versions.
- Correct firmware, 9.2(1) or a later version, is installed.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `max-dn max-no-of-directories [dual-line | octo-line]`
5. `timeouts busy seconds`
6. `end`

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>Enables privileged EXEC mode.  &lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong>  &lt;br&gt;Router&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>  &lt;br&gt;Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>call-manager-fallback</code></td>
<td>Enables Cisco Unified SRST support and enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>  &lt;br&gt;Router(config)# call-manager-fallback</td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action

### Step 4

```
max-dn max-no-of-directories [dual-line | octo-line]
```

**Example:**

Router(config-cm-fallback)# max-dn 10 octo-line

**Purpose:**
Sets the maximum possible number of directory numbers or virtual voice ports that can be supported by a router and enables dual-line mode, octo-line mode, or both modes.

- **max-no-of-directories**—Maximum number of directory numbers or virtual voice ports supported by the router. The maximum possible number is platform-dependent. The default is 0 directory numbers and 1 channel per virtual port.
- **dual-line**—(Optional) Sets all Cisco Unified IP phones connected to a Cisco Unified SRST router to one virtual voice port with two channels.
- **octo-line**—(Optional) Sets all Cisco Unified IP phones connected to a Cisco Unified SRST router to one virtual voice port with eight channels.

### Step 5

```
timeouts busy seconds
```

**Example:**

Router(config-cm-fallback)# timeouts busy 10

**Purpose:**
Sets the timeout value for call transfers to busy destinations.

- **seconds**—Number of seconds after connection to a busy destination before a transferred call is disconnected. Range is 0 to 30. Default: 10.

### Step 6

```
end
```

**Example:**

Router(config-cm-fallback)# end

**Purpose:**
Exits configuration mode and enters privileged EXEC mode.
Troubleshooting

To troubleshoot your Cisco Unified SRST configuration, use the following commands:

- To set keepalive debugging for Cisco IP phones, use the `debug ephone keepalive` command.
- To set registration debugging for Cisco IP phones, use the `debug ephone register` command.
- To set state debugging for Cisco IP phones, use the `debug ephone state` command.
- To set detail debugging for Cisco IP phones, use the `debug ephone detail` command.
- To set error debugging for Cisco IP phones, use the `debug ephone error` command.
- To set call statistics debugging for Cisco IP phones, use the `debug ephone statistics` command.
- To provide voice-packet-level debugging and to display the contents of one voice packet in every 1024 voice packets, use the `debug ephone pak` command.
- To provide raw low-level protocol debugging display for all SCCP messages, use the `debug ephone raw` command.

For further debugging, see *Cisco IOS Debug Command Reference*.

How to Set Up Cisco IP Communicator for Cisco Unified SRST

Cisco IP Communicator is a software-based application that delivers enhanced telephony support on personal computers. Cisco IP Communicator appears on a user’s computer monitor as a graphical, display-based IP phone with a color screen, a keypad, feature buttons, and soft keys.

For information about operation, see the Cisco IP Communicator online help and user documentation.

Prerequisites

You should have the following before you begin this task:

- IP address of the Cisco Unified CM (Call Manager) TFTP server
- IP address of the Cisco Unified SRST TFTP server
- Headset with microphone for your PC (Optional; you can use PC internal speakers and microphone)

---

**Step 1**  
Download the latest version of the Cisco IP Communicator software and install it on your PC. The software is available for download at [http://www.cisco.com/cisco/web/download/index.html](http://www.cisco.com/cisco/web/download/index.html).

a. Click **Voice and Unified Communication**.

b. Click **IP Telephony**.

c. Click **IP Phones**.

d. Click **Cisco IP Communicator**.

**Step 2**  
(Optional) Attach a headset to your PC.

**Step 3**  
Start the Cisco IP Communicator software application.
**Where to Go Next**

The next step is configuring Cisco Unified IP Phones using SIP. For more information, see the “**” section on page 165.

For additional information, see the “Additional References” section on page 29.
Setting Up Cisco Unified IP Phones using SIP

Session Initiation Protocol (SIP) registrar functionality in Cisco IOS software is an essential part of Cisco Unified SIP Survivable Remote Site Telephony (SRST). According to RFC 3261, a SIP registrar is a server that accepts Register requests and is typically collocated with a proxy or redirect server. A SIP registrar may also offer location services.

Contents

- Prerequisites for Configuring the SIP Registrar, page 165
- Restrictions for Configuring the SIP Registrar, page 165
- Information About Configuring the SIP Registrar, page 165
- How to Configure the SIP Registrar, page 166
- Where to Go Next, page 180

Prerequisites for Configuring the SIP Registrar

Complete the prerequisites documented in the “Prerequisites for Configuring Cisco Unified SIP SRST” section on page 9 section in “Cisco Unified SRST Feature Overview” section on page 1.

Restrictions for Configuring the SIP Registrar

See the restrictions documented in the “Restrictions for Configuring Cisco Unified SIP SRST” section on page 10 section in “Cisco Unified SRST Feature Overview” section on page 1.

Information About Configuring the SIP Registrar

Cisco Unified SIP SRST provides backup to an external SIP call control (IP-PBX) by providing basic registrar and call handling services. These services are used by a SIP IP phone in the event of a WAN connection outage when the SIP phone is unable to communicate with its primary SIP proxy. The Cisco Unified SIP SRST device also provides PSTN gateway access for placing and receiving PSTN calls.

Cisco Unified SIP SRST works for the following types of calls:
How to Configure the SIP Registrar

This section contains the following procedures:

- Configuring the SIP Registrar, page 166 (required)
- Configuring Backup Registrar Service to SIP Phones, page 168 (required)
- Configuring Backup Registrar Service to SIP Phones (Using Optional Commands), page 172 (optional)
- Verifying SIP Registrar Configuration, page 175 (optional)
- Verifying Proxy Dial-Peer Configuration, page 177 (optional)

Configuring the SIP Registrar

The local SIP gateway that becomes the SIP registrar acts as a backup SIP proxy and accepts SIP Register messages from SIP phones. It becomes a location database of local SIP IP phones.

A registrar accepts SIP Register requests and dynamically builds VoIP dial peers, allowing the Cisco IOS voice gateway software to route calls to SIP phones.

If a SIP Register request has a Contact header that includes a DNS address, the Contact header is resolved before the contact is added to the SIP registrar database. This is done because during a WAN failure (and the resulting Cisco Unified SIP SRST functionality), DNS servers may not be available.

SIP registrar functionality is enabled with the following configuration. By default, Cisco Unified SIP SRST is not enabled and cannot accept SIP Register messages. The following configuration must be set up to accept incoming SIP Register messages.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `allow-connections sip to sip`
5. `sip`
6. `registrar server [expires [max sec] [min sec]]`
### 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 voice service configuration mode. |
| **Example:**  
  Router(config)# voice service voip | |
| **Step 4** allow-connections sip to sip | Allows connections from SIP to SIP endpoints. |
| **Example:**  
  Router(config-voi-srv)# allow-connections sip to sip | |
| **Step 5** sip | Enters SIP configuration mode. |
| **Example:**  
  Router(config-voi-srv)# sip | |
How to Configure the SIP Registrar

What to Do Next

For incoming SIP Register messages to be successfully accepted, users must also set up a voice register pool. See the “Configuring Backup Registrar Service to SIP Phones” section on page 168.

Configuring Backup Registrar Service to SIP Phones

Backup registrar service to SIP IP phones can be provided by configuring a voice register pool on SIP gateways. The voice register pool configuration provides registration permission control and can also be used to configure some dial-peer attributes that are applied to the dynamically created VoIP dial peers when SIP phone registrations match the pool. The following call types are supported:

- SIP IP phone to or from:
  - Local PSTN
  - Local analog FXS phones
  - Local SIP IP phone

The commands in the configuration below provide registration permission control and set up a basic voice register pool. The pool gives users control over which registrations are accepted by a Cisco Unified SIP SRST device and which can be rejected. Registrations that match this pool create VoIP SIP dial peers with the dial-peer attributes set to these configurations. Although only the `id` command is mandatory, this configuration example shows basic functionality.

For command-level information, see the appropriate command page in Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions).
Prerequisites

- The SIP registrar must be configured before a voice register pool is set up. See the “Configuring the SIP Registrar” section on page 166 for complete instructions.

Restrictions

- The `id` command identifies the individual SIP IP phone or sets of SIP IP phones that are to be configured. Thus, the `id` command configured in Step 5 is required and must be configured before any other voice register pool commands. When the `mac address` keyword and argument are used, the IP phone must be in the same subnet as that of the router’s LAN interface, such that the phone’s MAC address is visible in the router’s Address Resolution Protocol (ARP) cache. Once a MAC address is configured for a specific voice register pool, remove the existing MAC address before changing to a new MAC address.

- Proxy dial peers are autogenerated dial peers that route all calls from the PSTN to Cisco Unified SIP SRST. When a SIP phone registers to Cisco Unified SIP SRST and the `proxy` command is enabled, two dial peers are automatically created. The first dial peer routes to the proxy, and the second (or fallback) dial peer routes to the SIP phone. The same functionality can also be achieved with the appropriate creation of static dial peers (manually creating dial peers that point to the proxy). Proxy dial peers can be monitored to one proxy IP address, only. That is, only one proxy from a voice registration pool can be monitored at a time. If more than one proxy address needs to be monitored, you must manually create and configure additional dial peers.

`Note`

To monitor SIP proxies, the `call fallback active` command must be configured, as described in Step 3.

SUMMARY STEPS

1. enable
2. configure terminal
3. call fallback active
4. voice register pool `tag`
5. `id` `{network address | ip address | mac address}
6. preference `preference-order`
7. `proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]`
8. `voice-class codec `tag`
9. application `application-name`
10. 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> Router&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> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> call fallback active</td>
<td>(Optional) Enables a call request to fall back to alternate dial peers in case of network congestion.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call fallback active</td>
<td>• This command is used if you want to monitor the proxy dial peer and fallback to the next preferred dial peer. For full information on the call fallback active command, see PSTN Fallback Feature.</td>
</tr>
<tr>
<td><strong>Step 4</strong> voice register pool tag</td>
<td>Enters voice register pool configuration mode for SIP phones.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice register pool 12</td>
<td>• Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td><strong>Step 5</strong> id {network address mask</td>
<td>mask</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# id network 172.16.0.0 mask 255.255.0.0</td>
<td>• network address mask mask: The network address mask mask keyword/argument combination is used to accept SIP Register messages for the indicated phone numbers from any IP phone within the indicated IP subnet.</td>
</tr>
<tr>
<td></td>
<td>• ip address mask mask: The ip address mask mask keyword/argument combination is used to identify an individual phone.</td>
</tr>
<tr>
<td></td>
<td>• mac address: MAC address of a particular Cisco Unified IP Phone.</td>
</tr>
<tr>
<td><strong>Step 6</strong> preference preference-order</td>
<td>Sets the preference order for the VoIP dial peers to be created. Range is from 0 to 10. Default is 0, which is the highest preference.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# preference 2</td>
<td>• The preference must be greater (lower priority) than the preference configured with the preference keyword in the proxy command.</td>
</tr>
</tbody>
</table>
### Chapter 7  Setting Up Cisco Unified IP Phones using SIP

#### How to Configure the SIP Registrar

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td></td>
</tr>
<tr>
<td>proxy ip-address [preference value] [monitor probe {icmp-ping</td>
<td>rtr} [alternate-ip-address]]</td>
</tr>
<tr>
<td></td>
<td>• <em>ip-address</em>: IP address of the SIP proxy.</td>
</tr>
<tr>
<td></td>
<td>• <em>preference value</em>: (Optional) Defines the preference of the proxy dial peers that are created. The preference must be less (higher priority) than the preference configured with the <em>preference</em> command. The range is from 0 to 10. The highest preference is 0. There is no default.</td>
</tr>
<tr>
<td></td>
<td>• <em>monitor probe</em>: (Optional) Enables monitoring of proxy dial peers.</td>
</tr>
<tr>
<td></td>
<td>• <em>icmp-ping</em>: Enables monitoring of proxy dial peers using ICMP ping.</td>
</tr>
<tr>
<td></td>
<td>• <em>rtr</em>: Enables monitoring of proxy dial peers using RTR probes.</td>
</tr>
<tr>
<td></td>
<td>• <em>alternate-ip-address</em>: (Optional) Enables monitoring of alternate IP addresses other than the proxy address. For example, to monitor a gateway front end to a SIP proxy.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-register-pool)# proxy 10.2.161.187 preference 1</td>
<td></td>
</tr>
</tbody>
</table>

| Step 8            | Sets the voice class codec parameters. The *tag* argument is a codec group number between 1 and 10000. |
| voice-class codec tag |         |
| Example:          |         |
| Router(config-register-pool)# voice-class codec 15 |         |

| Step 9            | (Optional) Selects the session-level application on the VoIP dial peer. Use the *application-name* argument to define a specific interactive voice response (IVR) application. |
| application application-name |         |
| Example:          |         |
| Router(config-register-pool)# application SIP.App |         |

| Step 10           | Returns to privileged EXEC mode. |
| end               |         |
| Example:          |         |
| Router(config-register-pool)# end |         |

### What to Do Next

There are several more voice register pool commands that add functionality, but that are not required. See the “Configuring Backup Registrar Service to SIP Phones (Using Optional Commands)” section on page 172 for these commands.
How to Configure the SIP Registrar

Configuring Backup Registrar Service to SIP Phones (Using Optional Commands)

The prior configurations set up a basic voice register pool. The configuration in this procedure adds optional attributes to increase functionality.

Prerequisites

- Prerequisites as described in the “Configuring Backup Registrar Service to SIP Phones” section on page 168.
- Configuration of the required commands as described in the “Configuring Backup Registrar Service to SIP Phones” section on page 168.
- Before configuring the 'alias' command, translation rules must be set using the translate-outgoing (voice register pool) command.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool tag
4. translation-profile outgoing profile-tag
5. alias tag pattern to target [preference value]
6. cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [- ending-number] | default}
7. incoming called-number [number]
8. number tag number-pattern {preference value} [huntstop]
9. dtmf-relay [cisco-rtp] [rtp-nte] [sip-notify]
10. 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>• 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>
</tbody>
</table>

Router> enable
Router# configure terminal
## How to Configure the SIP Registrar

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> voice register pool <strong>tag</strong></td>
<td>Enters voice register pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice register pool 12</td>
<td>- Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td><strong>Step 4</strong> translation-profile outgoing <strong>profile-tag</strong></td>
<td>Use this command to apply the translation profile to a specific directory number or to all directory numbers on a SIP phone.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# voice translation-rule 1 voice translation-profile 1 translate called 1 voice register pool xxx translation-profile outgoing 1</td>
<td>- <strong>Profile-tag:</strong> Translation profile name to handle translation to outgoing calls.</td>
</tr>
<tr>
<td><strong>Step 5</strong> alias <strong>tag</strong> <strong>pattern</strong> to <strong>target</strong> [<strong>preference</strong> <strong>value</strong>]</td>
<td>Allows Cisco Unified SIP IP Phones to handle inbound PSTN calls to telephone numbers that are unavailable when the main proxy is not available. The keywords and arguments are defined as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# alias 1 94... to 91011 preference 8</td>
<td>- <strong>tag:</strong> Number from 1 to 5 and the distinguishing factor when there are multiple alias commands.</td>
</tr>
<tr>
<td></td>
<td>- <strong>pattern:</strong> The prefix number; matches the incoming telephone number and may include wildcards.</td>
</tr>
<tr>
<td></td>
<td>- <strong>to:</strong> Connects the tag number pattern to the alternate number.</td>
</tr>
<tr>
<td></td>
<td>- <strong>target:</strong> The target number; an alternate telephone number to route incoming calls to match the number pattern.</td>
</tr>
<tr>
<td></td>
<td>- <strong>preference value:</strong> (Optional) Assigns a dial-peer preference value to the alias. The value argument is the value of the associated dial peer, and the range is from 1 to 10. There is no default.</td>
</tr>
</tbody>
</table>
Chapter 7  Setting Up Cisco Unified IP Phones using SIP

How to Configure the SIP Registrar

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>Configures a class of restriction (COR) on the VoIP dial peers associated with directory numbers. COR specifies which incoming dial peers can use which outgoing dial peers to make a call. Each dial peer can be provisioned with an incoming and outgoing COR list. The keywords and arguments are defined as follows:</td>
</tr>
<tr>
<td>cor (incoming</td>
<td>outgoing) cor-list-name (cor-list-number starting-number [- ending-number]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-register-pool)# cor incoming call91 1 91011</td>
</tr>
</tbody>
</table>

- **incoming**: COR list to be used by incoming dial peers.
- **outgoing**: COR list to be used by outgoing dial peers.
- **cor-list-name**: COR list name.
- **cor-list-number**: COR list identifier. The maximum number of COR lists that can be created is four, comprised of incoming or outgoing dial peers.
- **starting-number**: Start of a directory number range, if an ending number is included. Can also be a standalone number.
- **(Optional) Indicator that a full range is configured.**
- **ending-number**: (Optional) End of a directory number range.
- **default**: Instructs the router to use an existing default COR list.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>incoming called-number [number]</th>
<th>Applies incoming called parameters to dynamically created dial peers. The <em>number</em> argument is optional and indicates a sequence of digits that represent a phone number prefix.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-register-pool)# incoming called-number 308</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>number tag number-pattern {preference value}</th>
<th>Indicates the E.164 phone numbers that the registrar permits to handle the Register message from the Cisco Unified SIP IP Phone. The keywords and arguments are defined as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-register-pool)# number 1 50.. preference 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tag: Number from 1 to 10 and the distinguishing factor when there are multiple number commands.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>number-pattern: Phone numbers (including wildcards and patterns) that are permitted by the registrar to handle the Register message from the SIP IP phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>preference value: (Optional) Defines the number list preference order.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>huntstop: (Optional) Stops hunting if the dial peer is busy.</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure the SIP Registrar

**Examples**

The following partial output from the `show running-config` command shows that voice register pool 12 is configured to accept all registrations from SIP IP phones with extension number 50xx from the 172.16.0.0/16 network. Autogenerated dial peers for registrations that match pool 12 have attributes configured in this pool.

```
voice register pool 12
  id network 172.16.0.0 mask 255.255.0.0
  number 1 50.. preference 2
  application SIP.app
  preference 2
  incoming called-number
  cor incoming allowall default
  translate-outgoing called 1
  voice-class codec 1

Verifying SIP Registrar Configuration

To help you troubleshoot a SIP registrar and voice register pool, perform the following steps.

**SUMMARY STEPS**

1. debug voice register errors
2. debug voice register events
3. show sip-ua status registrar
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> debug voice register errors</td>
<td>Use this command to debug errors that happen during registration. If there are no voice register pools configured for a particular registration request, the message “Contact doesn’t match any pools” is displayed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# debug voice register errors</td>
<td></td>
</tr>
<tr>
<td>Apr 22 11:52:54.523 PDT: VOICE_REG_POOL: Contact doesn’t match any pools</td>
<td></td>
</tr>
<tr>
<td>Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Register request for (33015) from (10.2.152.39)</td>
<td></td>
</tr>
<tr>
<td>Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Contact doesn’t match any pools.</td>
<td></td>
</tr>
<tr>
<td>Apr 22 11:52:54.559 PDT: VOICE_REG_POOL: Register request for (33017) from (10.2.152.39)</td>
<td></td>
</tr>
<tr>
<td>Apr 22 11:53:04.559 PDT: VOICE_REG_POOL: Maximum registration threshold for pool(3) hit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> debug voice register events</td>
<td>Using the <code>debug voice register events</code> command should suffice to display registration activity. Registration activity includes matching of pools, registration creation, and automatic creation of dial peers. For more details and error conditions, you can use the <code>debug voice register errors</code> command. The phone number 91011 registered successfully, and <strong>type 1</strong> is reported, which means there is a pre-existing VoIP dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# debug voice register events</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Contact matches pool 1</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) contact(192.168.0.2) add to contact table</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) exists in contact table</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: contact(192.168.0.2) exists in contact table, ref updated</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Created dial-peer entry of type 1</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Registration successful for 91011, registration id is 257</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show sip-ua status registrar</td>
<td>Use this command to display all the SIP endpoints currently registered with the contact address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show sip-ua status registrar</td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td>destination</td>
</tr>
<tr>
<td>====</td>
<td>===========</td>
</tr>
<tr>
<td>91021</td>
<td>192.168.0.3</td>
</tr>
<tr>
<td>91011</td>
<td>192.168.0.2</td>
</tr>
<tr>
<td>95021</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95012</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95011</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95500</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>94011</td>
<td>10.2.161.40</td>
</tr>
<tr>
<td>94500</td>
<td>10.2.161.40</td>
</tr>
</tbody>
</table>
Verifying Proxy Dial-Peer Configuration

To use the `icmp-ping` keyword with the `proxy` command to assist in troubleshooting proxy dial peers, perform the following steps.

**SUMMARY STEPS**

1. `configure terminal`
2. `voice register pool tag`
3. `proxy ip-address [preference value] [monitor probe {icmp-ping | rtr}] [alternate-ip-address]`
4. `end`
5. `show voice register dial-peers`
6. `show dial-peer voice`
## How to Configure the SIP Registrar

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>voice register pool tag</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# voice register pool 1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>proxy ip-address [preference value] [monitor probe [icmp-ping</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-register-pool)# proxy 10.2.161.187 preference 1 monitor probe icmp-ping</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-register-pool)# end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show voice register dial-peers</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show voice register dial-peers dial-peer voice 40035 voip preference 5 destination-pattern 91011 session target ipv4:192.168.0.2 session protocol sipv2 voice-class codec 1 dial-peer voice 40036 voip preference 1 destination-pattern 91011 session target ipv4:10.2.161.187 session protocol sipv2 voice-class codec 1 monitor probe icmp-ping 10.2.161.187</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 6**

```
show dial-peer voice
```

**Example:**

```
Router# show dial-peer voice
VoiceOverIpPeer40036
peer type = voice, information type = voice, 
description = '',
tag = 40036, destination-pattern = '91011',
answer-address = '', preference=1,
CLID Restriction = None
CLID Network Number = '',
CLID Second Number sent
source carrier-id = '', target carrier-id = '',
source trunk-group-label = '', target
trunk-group-label = '',
numbering Type = 'unknown'
group = 40036, Admin state is up, Operation state is 
up,
incoming called-number = '', connections/maximum = 
0/unlimited,

! Default output for incoming called-number command
DTMF Relay = disabled,
modem transport = system,
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
! Default output for cor command
outgoing COR list:minimum requirement

! Default output for cor command
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translate-profile =''
disconnect-cause = 'no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4
oldAddrFamily 4
type = voip, session-target = 'ipv4:10.2.161.187',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip signaling DSCP = af31,
af video rsvp-none DSCP = af41,ip video rsvp-pass
DSCP = af41
ip video rsvp-fail DSCP = af41,
UDP checksum = disabled,
session-protocol = sipv2, session-transport = 
system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = 
best-effort,
req-qos audio def bandwidth = 64, req-qos audio max 
bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max
bandwidth = 0,
```

### Purpose

Use the `show dial-peer voice` command on dial peer 40036, and notice the monitor probe status.

### Note

Also highlighted is the output of the `cor` and `incoming called-number` commands.
The next step is configuring incoming and outgoing calls for Cisco Unified SRST. For more information, see the “Configuring Call Handling” section on page 183.

For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
Configuring Call Handling

This chapter describes how to configure Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) for incoming and outgoing calls for SCCP phones.

This chapter also describes support for standardized RFC 3261 features for SIP phones. Features include call blocking and call forwarding.

Note: Configuring Call Handling for SIP phones applies to versions 4.0 and 3.4 only.

Contents

- Prerequisites for Configuring SIP SRST Features Using Back-to-Back User Agent Mode, page 184
- Restrictions for Configuring SIP SRST Features Using Back-to-Back User Agent Mode, page 184
- Information About Configuring SCCP SRST Call Handling, page 184
- Information About Configuring SIP SRST Features Using Back-to-Back User Agent Mode, page 185
- How to Configure Cisco Unified SCCP SRST, page 187
- How to Configure Cisco Unified SIP SRST, page 224
- How to Configure Optional Features, page 234
- Configuration Examples for Call Handling, page 236
- Where to Go Next, page 237
Prerequisites for Configuring SIP SRST Features Using Back-to-Back User Agent Mode

- Complete the prerequisites documented in the “Prerequisites for Configuring Cisco Unified SIP SRST” section on page 9 in the “Cisco Unified SRST Feature Overview” section on page 1.
- Configure the SIP registrar. The SIP registrar gives users control of accepting or rejecting registrations. To configure acceptance of incoming SIP Register messages, see the section on page 165.

Restrictions for Configuring SIP SRST Features Using Back-to-Back User Agent Mode

- See the restrictions documented in the “Restrictions for Configuring Cisco Unified SIP SRST” section on page 10 in the “Cisco Unified SRST Feature Overview” section on page 1.

Information About Configuring SCCP SRST Call Handling

Cisco Unified SRST offers a smaller set of call handling capabilities than Cisco Unified CM, and much of the configuration for these features involves enabling existing Cisco Unified CM or Cisco Unified IP Phone settings.

- H.323 VoIP Call Preservation Enhancements for WAN Link Failures, page 184
- Toll Fraud Prevention, page 185

H.323 VoIP Call Preservation Enhancements for WAN Link Failures

H.323 VoIP call preservation enhancements for WAN link failures sustain connectivity for H.323 topologies where signaling is handled by an entity, such as Cisco Unified Communications Manager, that is different from the other endpoint and brokers signaling between the two connected parties.

Call preservation is useful when a gateway and the other endpoint (typically a Cisco Unified IP phone) are collocated at the same site and call agent is remote and therefore more likely to experience connectivity failures.

For configuration information see “Configuring H.323 Gateways” chapter in Cisco IOS H.323 Configuration Guide, Release 12.4T.
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. For more information about Toll Fraud Prevention, see Toll Fraud Prevention in Cisco Unified Communications Manager Express System Administration Guide.

Information About Configuring SIP SRST Features Using Back-to-Back User Agent Mode

A Cisco Unified SRST system can now support SIP phones with standard-based RFC 3261 feature support locally and across SIP WAN networks. With Cisco Unified SIP SRST, SIP phones can place calls across SIP networks with similar features, as SCCP phones do. For example, most SCCP phone features such as caller ID, speed dial, and redial are supported now on SIP networks, which gives users the opportunity to choose SCCP or SIP.

Cisco Unified SIP SRST also uses a back-to-back user agent (B2BUA), which is a separate call agent that has more features than Cisco SIP SRST 3.0, which used a redirect server that only accepted and forwarded calls. The main advantage of a B2BUA call agent is in call forwarding, because it forwards calls on behalf of the phone. In addition, it maintains a presence as call middleman in the call path.

Cisco SIP SRST 3.4 supports the following call combinations:

- SIP phone to SIP phone
- SIP phone to PSTN / router voice port
- SIP phone to SCCP phone

Cisco Unified SIP SRST and Cisco SIP Communications Manager Express Feature Crossover

The voice register dn, voice register global and voice register pool configuration mode commands are accessible in both Cisco Unified SIP CME and Cisco Unified SIP SRST modes of operation. However, not all of the commands within these modes are intended for use in SIP SRST mode. Table 8-1 provides a summary guide to which commands are relevant to the CME or SRST modes of operation.

For more detailed information, refer to the command reference pages for each of the individual commands.

Note: Table 8-1 is not all-inclusive; additional commands may exist.
### Table 8-1 Version 3.4 New or Enhanced Commands for Cisco Unified SRST and Cisco Unified CME (Sorted by Configuration Mode)

<table>
<thead>
<tr>
<th>Command</th>
<th>Dial Peer</th>
<th>Voice Register Mode</th>
<th>Configurable for Cisco Unified (SIP) CME and Cisco Unified SIP SRST</th>
<th>Applicable to Cisco Unified (SIP) CME Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>after-hour exempt</td>
<td>X</td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>auto-answer</td>
<td></td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>call forward</td>
<td>X</td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>huntstop</td>
<td>X</td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>label</td>
<td></td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>name</td>
<td></td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>number</td>
<td>X</td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>preference</td>
<td>X</td>
<td>dn</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>application</td>
<td>X</td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>authenticate</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>create</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>date-format</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>dst</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>external ring</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>file</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>hold-alert</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>load</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>logo</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>max-dn</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>max-pool</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>max-redirect</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>mode</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>mwi</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>reset</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>tftp-path</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>timezone</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>upgrade</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>url</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>voicemail</td>
<td></td>
<td>global</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>after-hour exempt</td>
<td>X</td>
<td>pool</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>application</td>
<td>X</td>
<td>pool</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>call-forward</td>
<td></td>
<td>pool</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>call-waiting</td>
<td></td>
<td>pool</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>codec</td>
<td>X</td>
<td>pool</td>
<td>X</td>
<td>—</td>
</tr>
</tbody>
</table>
How to Configure Cisco Unified SCCP SRST

Setting up call handling involves the following set of tasks:

- Configuring Incoming Calls, page 188
- Configuring Outgoing Calls, page 207
- Configuring Call Blocking Based on Time of Day, Day of Week, or Date, page 228
Configuring Incoming Calls

Incoming call configuration can include the following tasks:

- Call Forwarding and Rerouting
  - Configuring Call Forwarding During a Busy Signal or No Answer, page 188 (Optional)
  - Configuring Call Rerouting, page 190 (Optional)
  - Configuring Call Pickup, page 193 (Optional)
  - Configuring Transfer Digit Collection Method, page 196
- Phone Number Conversion and Translation
  - Configuring Global Prefixes, page 197 (Optional)
  - Enabling Digit Translation Rules, page 199 (Optional)
  - Enabling Translation Profiles, page 200 (Optional)
  - Verifying Translation Profiles, page 203 (Optional)
- Hunting and Ringing Timeout Behavior
  - Configuring Dial-Peer and Channel Hunting, page 204 (Optional)
  - Configuring Busy Timeout, page 205 (Optional)
  - Configuring the Ringing Timeout Default, page 206 (Optional)

Configuring Call Forwarding During a Busy Signal or No Answer

Incoming calls that reach a busy signal or go unanswered during Cisco Unified CM fallback can be configured to be forwarded to one or more E.164 numbers.

SUMMARY STEPS

1. call-manager-fallback
2. call-forward busy directory-number
3. call-forward noan directory-number timeout seconds
4. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>call-forward busy directory-number</td>
<td>Configures call forwarding to another number when the Cisco IP phone is busy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-cm-fallback)# call-forward busy 50..</td>
<td>- <em>directory-number</em>: Selected directory number representing a fully qualified E.164 number. This number can contain “.” wildcard characters that correspond to the right-justified digits in the directory number extension.</td>
</tr>
<tr>
<td>3</td>
<td>call-forward noan directory-number timeout seconds</td>
<td>Configures call forwarding to another number when no answer is received from the Cisco IP phone.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-cm-fallback)# call-forward noan 5005 timeout 10</td>
<td>- <em>directory-number</em>: Selected directory number representing a fully qualified E.164 number or a local extension number. This number can contain “.” wildcard characters that correspond to the right-justified digits in the directory number extension.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <em>timeout seconds</em>: Sets the waiting time, in seconds, before the call is forwarded to another phone. The seconds range is from 3 to 60000.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example forwards calls to extension number 5005 when an incoming call reaches a busy or unattended IP phone extension number. Incoming calls will ring for 15 seconds before being forwarded to extension 5005.

```
call-manager-fallback
  call-forward busy 5005
  call-forward noan 5005 timeout 15
```

The following example transforms an extension number for call forwarding when the extension number is busy or unattended. The `call-forward busy` command has an argument of 50., which prepends the digits 50 to the last two digits of the called extension. The resulting extension is the number to which incoming calls are forwarded when the original extension number is busy or unattended. For instance, an incoming call to the busy extension 6002 will be forwarded to extension 5002, and an incoming call to the busy extension 3442 will be forwarded to extension 5042. Incoming calls will ring for 15 seconds before being forwarded.

```
call-manager-fallback
  call-forward busy 50..
  call-forward noan 50.. timeout 15
```
### Configuring Call Rerouting

We recommend the `alias` command, which obsoletes the `default-destination` command, instead of the `default-destination` command.

The `alias` command provides a mechanism for rerouting calls to telephone numbers that are unavailable during fallback. Up to 50 sets of rerouting alias rules can be created for calls to telephone numbers that are unavailable during Cisco Unified Communications Manager fallback. Sets of alias rules are created using the `alias` command. An alias is activated when a telephone registers that has a phone number matching a configured `alternate-number` alias. Under that condition, an incoming call is rerouted to the alternate number. The `alternate-number` argument can be used in multiple `alias` commands, allowing you to reroute multiple different numbers to the same target number.

The configured `alternate-number` must be a specific E.164 phone number or extension that belongs to an IP phone registered on the Cisco Unified SRST router. When an IP phone registers with a number that matches an `alternate-number`, an additional POTS dial peer is created. The destination pattern is set to the initial configured `number-pattern`, and the POTS dial peer voice port is set to match the voice port associated with the `alternate-number`.

If other IP phones register with specific phone numbers within the range of the initial `number-pattern`, the call is routed back to the IP phone rather than to the `alternate-number` (according to normal dial-peer longest-match, preference, and huntstop rules).

### Call Forward Destination

The `cfw` keyword allows you to configure a call forward destination for calls that are busy or not answered. Call forward no answer is defined as when the phone rings for a user configurable amount of time, the call is not answered, and is forwarded to the configured destination. Call forward busy and call forward no answer can be configured to a set string and override globally configured call forward settings.

Globally configured settings are selected under call-manager-fallback and apply to all phones that register for SRST service.

You can also create a specific call forwarding path for a particular number. The benefit of using the `cfw` keyword is that during SRST, you can reroute calls from otherwise unreachable numbers onto phones that are available. Basic hunt groups can be established with call-forwarding rules so that if the first SRST phone is busy, you can forward the call to a second SRST phone.

The `cfw` keyword also allows you to alias a phone number to itself, permitting setting of per-phone number forwarding. An example of aliasing a number to itself follows. If a phone registers with extension 1001, a dial peer that routes calls to the phone is automatically created for 1001. If the call-manager-fallback dial-peer preference (set with the `max-dn` command) for this initial dial peer is set to 2, the dial peer uses 2 as its preference setting.

Then, use the `alias` command to alias the phone number to itself:

```
alias 1 1001 to 1001 preference 1 cfw 2001 timeout 20
```
In this example, you have created a second dial peer for 1001 to route calls to 1001, but that has preference 1 and call forwarding to 2001. Because the preference on the dial peer created by the **alias** command is now a lower numeric value than the preference that the dial peer first created, all calls come initially to the dial peer created by the **alias** command. In that way, they are subject to the forward as set by the **alias** command, instead of any call forwarding that may have been set globally.

**Huntstop on an Individual Alias**

The alias **huntstop** keyword is relevant only if you have also set the global **no huntstop** command under call-manager-fallback. Also, you may need to set the global **no huntstop** if you have multiple **alias** commands with the same **number-pattern** and you want to enable hunting on busy between the aliases. That is, one alias for **number-pattern** is tried, and then if that phone is busy, the second alias for **number-pattern** is tried.

The alias **huntstop** keyword allows you to turn huntstop behavior back on for an individual alias, if huntstop is turned off globally by the **no huntstop** command. Setting the **huntstop** keyword on an individual alias stops hunting at the alias, making the alias the final member of the hunt sequence.

**SUMMARY STEPS**

1. **call-manager-fallback**
2. **alias** `tag number-pattern to alternate-number [preference preference-value] [cfw number timeout timeout-value] [huntstop]`
3. **max-dn** `max-directory-numbers [dual-line] [preference preference-order]`
4. **end**
5. **show dial-peer voice summary**
### 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>call-manager-fallback</strong>&lt;br&gt;Example: &lt;br&gt;Router(config)# call-manager-fallback</td>
</tr>
</tbody>
</table>
| **Step 2** | **alias tag number-pattern to alternate-number [preference preference-value] [cfw number timeout timeout-value] [huntstop]**<br>Example: <br>Router(config-cm-fallback)# alias 1 60.. to 5001 preference 1 cfw 2000 timeout 10 | Creates a set rules for rerouting calls to sets of phones that are unavailable during Cisco Unified CM fallback.  
- **tag**: Identifier for alias rule range. The range is from 1 to 50. 
- **number-pattern**: Pattern to match the incoming telephone number. This pattern may include wildcards. 
- **to**: Connects the tag number pattern to the alternate number. 
- **alternate-number**: Alternate telephone number to route incoming calls to match the number pattern. The alternate number has to be a specific extension that belongs to an IP phone that is actively registered on the Cisco Unified SRST router. The alternate telephone number can be used in multiple **alias** commands. 
- **preference preference-value** (Optional). Assigns a dial-peer preference value to the alias. The preference value of the associated dial peer is from 0 to 10. Use with the **max-dn** command. 
- **cfw number** (Optional). The cfw keyword allows users to set call forward busy and call forward no answer to a set string and override globally configured call forward settings. 
- **timeout timeout-value** (Optional). Sets the ring no-answer timeout duration for call forwarding, in seconds. Range is from 3 to 60000. 
- **huntstop** (Optional). Stops call hunting after trying the alternate number. |
| **Step 3** | **max-dn max-directory-numbers [dual-line] [preference preference-order]**<br>Example: <br>Router(config-cm-fallback)# max-dn 10 preference 2 | Sets the maximum possible number of directory numbers or virtual voice ports that can be supported by a router and sets the global preference for creating the VoIP dial peers for all directory numbers that are associated with the primary number.  
- Using the **max-dn** command sets the preference for the default dial peers created with the **alias** command. 
- When configuring call rerouting, set the **max-dn preference** to a higher numeric preference than the preference that was set with the **alias** command. |
How to Configure Cisco Unified SCCP SRST

**Examples**

The following example sets the `preference` keyword in the `alias` command to a lower preference value that the preference value created by the `max-dn` command. Setting the value lower allows the `cfw` keyword to take effect. The incoming call to extension 1000 hunts to alias because it has a lower preference, and no-answer/busy calls to 1000 are forwarded to 2000. All incoming calls to other extensions in SRST mode are forwarded to 3000 after 10 seconds.

```
call-manager-fallback
alias 1 1000 to 1000 preference 1 cfw 2000 timeout 10
max-dn 10 preference 2
call-forward busy 3000
call-forward noan 3000 timeout 10
```

**Configuring Call Pickup**

Configuring the `pickup` command enables the PickUp soft key on all SRST phones. You can then press the PickUp key and answer any currently ringing IP phone that has a DID called number that matches the configured `telephone-number`. This command does not enable the Group PickUp (GPickUp) soft key.

When a user presses the PickUp soft key, SRST searches through all the SRST phones to find a ringing call that has a called number that matches the configured `telephone-number`. When a match is found, the call is automatically forwarded to the extension number of the phone that requested the call pickup.

The SRST `pickup` command is designed to operate in a manner compatible with Cisco Unified Communications Manager.

**Note**

The default phone load on Cisco Unified Communications Manager, Release 4.0(1) for the Cisco 7905 andCisco 7912 IP phones does not enable the PickUp soft key during fallback. To enable the PickUp soft key on Cisco 7905 and Cisco 7912 IP phones, upgrade your default phone load to Cisco Unified CM, Version 4.0(1) Sr2. Alternatively, you can upgrade the phone load to `cmterm-7905g-sccp.3-3-8.exe` or `cmterm-7912g-sccp.3-3-8.exe`, respectively.

**SUMMARY STEPS**

1. `call-manager-fallback`
2. `no huntstop`
3. `alias tag number-pattern to alternate-number`
4. `pickup telephone-number`
5. `end`
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# call-manager-fallback</td>
</tr>
<tr>
<td><strong>Step 2</strong> no huntstop</td>
<td>Disables huntstop.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# no huntstop</td>
</tr>
<tr>
<td><strong>Step 3</strong> alias tag number-pattern to alternate-number</td>
<td>Creates a set rules for rerouting calls to sets of phones that are unavailable during Cisco Unified CM fallback.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# alias 1 8005550100 to 5001</td>
</tr>
<tr>
<td></td>
<td>- <em>tag:</em> Identifier for alias rule range. The range is from 1 to 50.</td>
</tr>
<tr>
<td></td>
<td>- <em>number-pattern:</em> Pattern to match the incoming telephone number. This pattern may include wildcards.</td>
</tr>
<tr>
<td></td>
<td>- <em>to:</em> Connects the tag number pattern to the alternate number.</td>
</tr>
<tr>
<td></td>
<td>- <em>alternate-number:</em> Alternate telephone number to route incoming calls to match the number pattern. The alternate number has to be a specific extension that belongs to an IP phone that is actively registered on the Cisco Unified SRST router. The alternate telephone number can be used in multiple alias commands.</td>
</tr>
<tr>
<td><strong>Step 4</strong> pickup telephone-number</td>
<td>Enables the PickUp soft key on all Cisco Unified IP Phones, allowing an external Direct Inward Dialing (DID) call coming into one extension to be picked up from another extension during SRST. The telephone-number argument is the telephone number to match an incoming called number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# pickup 8005550100</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# end</td>
</tr>
</tbody>
</table>

## Examples

The **pickup** command is best used with the **alias** command. The following partial output from the **show running-config** command shows the **pickup** command and the **alias** command configured to provide call routing for a pilot number of a hunt group:

```plaintext
call-manager-fallback
no huntstop
alias 1 8005550100 to 5001
alias 2 8005550100 to 5002
alias 3 8005550100 to 5003
alias 4 8005550100 to 5004
pickup 8005550100
```
When a DID incoming call to 800 555-0100 is received, the alias command routes the call at random to one of the four extensions (5001 to 5004). Because the pickup command is configured, if the DID call rings on extension 5002, the call can be answered from any of the other extensions (5001, 5003, 5004) by pressing the PickUp soft key.

The pickup command works by finding a match based on the incoming DID called number. In this example, a call from extension 5004 to extension 5001 (an internal call) does not activate the pickup command because the called number (5001) does not match the configured pickup number (800 555-0100). Thus, the pickup command distinguishes between internal and external calls if multiple calls are ringing simultaneously.

### Configuring Consultative Transfer

Before Cisco Unified SRST 4.3, the consultative transfer feature played a dial tone and collected dialed digits until the digits matched the pattern for consultative transfer, blind transfer, or PSTN transfer blocking. The after-hours blocking criteria was applied after the consultative transfer digit collection and pattern matching.

The new feature modifies the transfer digit-collection process to make it consistent with Cisco Unified Communications Manager. This feature is supported only if the transfer-system full-consult command (default) is specified in call-manager-fallback configuration mode and an idle line or channel is available for seizing, digit collection, and dialing.

Two lines are required for a consultative transfer. When the transferor party is an octo-line directory number, Cisco Unified SRST selects the next available idle channel on that directory number. If the maximum number of channels of the directory number are in use, another idle line on the transferor phone is considered. If the auto-line command is configured on the phone, the specified autoline (if idle) takes precedence over other nonauto lines. If no idle line is available on the transferor phone, a blind transfer is initiated instead of the consultative transfer.

During the consultative transfer, the transferor line to the transferee party is locked on the transferor phone to prevent it from being stolen by other phones sharing the same directory number. When the user presses the Transfer soft key for a consultative transfer, the Transfer soft key does not display while digits are being dialed and collected on this seized consultative transfer call leg. The method for consultative transfer pattern matching, blind transfer, PSTN transfer blocking, or after-hour blocking criteria remain the same although the manipulation after the matching is different. When the criteria for the blind transfer is met, Cisco Unified SMST terminates the consultative transfer call leg, informs the Cisco IOS software to transfer the call, and then terminates the original call bubble. The PARK FAC code is handled in the same way as by a new call which requires that a ten-second timer is applied by the Cisco IOS software.

The enhancement, by default, collects the transfer digits from the new call leg. If required, you can configure the system to collect the transfer digits from the original call leg. See the “Configuring Transfer Digit Collection Method” section on page 196.

The error handling for transfer failure because of transfer blocking or interdigit timer expiration remains. It includes displaying an error message on the prompt line and logging it if “debug ephone error” is enabled, playing a fast-busy or busy tone, and terminating the consultative transfer call leg.

No new configuration is required to support these enhancements.
Conference Calls

No configuration steps are required for these conference call enhancements.

**Single-Line Directory Number**
If the initiating party for the conference call is a single-line directory number and the phone has multiple directory numbers configured, the system selects another directory number’s idle channel for creating the conference. If there are multiple directory numbers (dual-line or single-line directory numbers) on the phone and each has calls on hold, the system prompts the user to select a line for the conference call.

**Dual-Line Directory Number**
If the initiating party for the conference call is a dual-line directory number, the system selects another idle channel from the dual-line directory number. If the selected channel has a call on hold, the conference operation will automatically select the hold channel and create the conference.

**Octo-Line Directory Number**
If the initiating party for the conference call is an octo-line directory number, the system selects an idle channel from the initiating party directory number and the user must establish a new call to complete the conference. If there is no idle channel on the same directory number, other idle directory numbers or channels on the same phone are not selected. If there are existing calls on hold on the other channels of the same directory number or other directory numbers, the user will not have the option to select them to join the conference. If there is no idle channel on the same directory number, the conference will abort with a No Line Available message.

Configuring Transfer Digit Collection Method

By default, transfer digits are collected from the new call leg. To change the transfer digit collection method, perform the following steps.

**Prerequisites for Cisco Unified SRST 4.3**

- Cisco Unified SRST 4.3
- Cisco Unified CM 6.0
- Cisco IOS Release 12.4(15)XZ

**Restrictions for Cisco Unified SRST 4.3**

- The Cisco 3200 Series Mobile Access Router does not support SRST.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `transfer-digit-collect {new-call | orig-call}`
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></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>transfer-digit-collect (new-call</td>
<td>orig-call)</td>
</tr>
<tr>
<td>Example:</td>
<td>• new-call: Digits are collected from the new call leg.</td>
</tr>
<tr>
<td>Router(config-cm-fallback)# transfer-digit-collect orig-call</td>
<td>• orig-call: Digits are collected from the original call-leg. This was the default behavior in versions before Cisco Unified SRST 4.3.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example shows the `transfer-digit-collect` method set to the legacy value of orig-call:

```
! call-manager-fallback
  transfer-digit-collect orig-call
!```

### Configuring Global Prefixes

The `dialplan-pattern` command creates a dial-plan pattern that specifies a global prefix for the expansion of abbreviated extension numbers into fully qualified E.164 numbers.

The `extension-pattern` keyword allows additional manipulation of abbreviated extension-number prefix digits. When this keyword and its argument are used, the leading digits of an extension pattern are stripped and replaced by the corresponding leading digits of the dial-plan pattern. This command can be used to avoid Direct Inward Dialing (DID) numbers like 408 555-0101 resulting in 4-digit extensions such as 0101.

Global prefixes are set with the `dialplan-pattern` command. Up to five dial-plan patterns can be created. The `no-reg` keyword provides dialing flexibility and prevents the E.164 numbers in the dial peer from registering to the gatekeeper. You have the option not to register numbers to the gatekeeper so that those numbers can be used for other telephony services.
### SUMMARY STEPS

1. **call-manager-fallback**
2. **dialplan-pattern** *tag* *pattern* *extension-length* *length* [*extension-pattern* *extension-pattern*] [*no-reg*]
3. **exit**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> dialplan-pattern <em>tag</em> <em>pattern</em> <em>extension-length</em> <em>length</em> [<em>extension-pattern</em> <em>extension-pattern</em>] [<em>no-reg</em>]</td>
<td>Creates a global prefix that can be used to expand the abbreviated extension numbers into fully qualified E.164 numbers</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# dialplan-pattern 1 4085550100 extension-length 3 extension-pattern 4..</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> This example maps all extension numbers 4xx to the PSTN number 40855501xx, so that extension 412 corresponds to 4085550112.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Examples

The following example shows how to create dial-plan pattern 1 for extension numbers 101 to 199 with the telephone prefix starting with 4085550. If the following example is set, the router will recognize that 4085550144 matches dial-plan pattern 1. It will use the extension-length keyword to extract the last three digits of the number 144 and present this as the caller ID for the incoming call.

```plaintext
call-manager-fallback
dialplan-pattern 1 40855501.. extension-length 3 no-reg
```

In the following example, the leading prefix digit for the 3-digit extension numbers is transformed from 0 to 4, so that the extension-number range becomes 400 to 499:

```plaintext
call-manager-fallback
dialplan-pattern 1 40855500.. extension-length 3 extension-pattern 4..
```

In the following example, the dialplan-pattern command creates dial-plan pattern 2 for extensions 801 to 899 with the telephone prefix starting with 4085559. As each number in the extension pattern is declared with the number command, two POTS dial peers are created. In the example, they are 801 (an internal office number) and 4085559001 (an external number).

```plaintext
call-manager-fallback
dialplan-pattern 2 40855590.. extension-length 3 extension-pattern 8..
```

Enabling Digit Translation Rules

Digit translation rules can be enabled during Cisco Unified CM fallback. Translation rules are a number-manipulation mechanism that performs operations such as automatically adding telephone area codes and prefix codes to dialed numbers.

Note

Digit translation rules have many applications and variations. For further information about them, see Cisco IOS Voice Configuration Library.

If you are running Cisco SRST 3.2 and later or Cisco Unified SRST 4.0 and later, use the configuration described in the “Enabling Translation Profiles” section on page 200 instead of using the translate command as described below. Translation Profiles are new to Cisco SRST 3.2 and provide added capabilities.

Translation rules can be used as follows:

- To manipulate the answer number indication (ANI) (calling number) or dialed number identification service (DNIS) (called number) digits for a voice call.
- To convert a telephone number into a different number before the call is matched to an inbound dial peer or before the call is forwarded by the outbound dial peer.

To view the translation rules configured for your system, use the show translation-rule command.

**SUMMARY STEPS**

1. call-manager-fallback
2. translate {called | calling} translation-rule-tag
3. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> translate (called</td>
<td>Applies a translation rule to modify the phone number dialed or received by any Cisco Unified IP Phone user while Cisco Unified CM fallback is active.</td>
</tr>
<tr>
<td>calling) translation-rule-tag</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# translate called 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example applies translation rule 10 to the calls coming into extension 1111. All inbound calls to 1111 will go to 2222 during Cisco Unified CM fallback.

```
translation-rule 10
rule 1 1111 2222 abbreviated
exit
call-manager-fallback
translate calling 10
```

The following is a sample configuration of digit translation rule 20, where the priority of the translation rule is 1 (the range is from 1 to 15) and the abbreviated representation of a complete number (1234) is replaced with the number 2345:

```
translation-rule 20
rule 1 1234 2345 abbreviated
exit
```

### Enabling Translation Profiles

Cisco SRST 3.2 and later and Cisco Unified SRST 4.0 and later support translation profiles. Translation profiles are the suggested way to allow you to group translation rules and provide instructions on how to apply the translation rules to the following:

- Called numbers
- Calling numbers
- Redirected called numbers
In the configuration below, the `voice translation-rule` and the `rule` command allow you to set and define how a number is to be manipulated. The `translate` command in voice translation-profile mode defines the type of number you are going to manipulate, such as a called, calling, or a redirecting number. Once you have defined your translation profiles, you can then apply the translation profiles in various places, such as dial peers and voice ports. For SRST, you apply your profiles in call-manager fallback mode.

Cisco IP phones support one incoming and one outgoing translation profile when in SRST mode.

**Note**

For Cisco SRST 3.2 and later versions and Cisco Unified SRST 4.0 and later versions, use the `voice translation-rule` and `translation-profile` commands shown below instead of the translation rule configuration described in the “Enabling Digit Translation Rules” section on page 199. Voice translation rules are a separate feature from translation rules. See the `voice translation-rule` command in *Cisco IOS Voice Command Reference* for more information and the *VoIP Gateway Trunk and Carrier Based Routing Enhancements* documentation for more general information on translation rules and profiles.

**SUMMARY STEPS**

1. `voice translation-rule number`
2. `rule precedence/match-pattern [replace-pattern]`
3. `exit`
4. `voice translation-profile name`
5. `translate {called | calling | redirect-called} voice-translation-rule-tag`
6. `exit`
7. `call-manager-fallback`
8. `translation-profile {incoming | outgoing} name`
9. `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></td>
</tr>
</tbody>
</table>
| `voice translation-rule number` | Defines a translation rule for voice calls and enters voice translation-rule configuration mode.  
  - `number`: Number that identifies the translation rule. Range is from 1 to 2147483647. |
| **Example:**      |         |
| `Router(config)# voice translation-rule 1` |         |
| **Step 2**        |         |
| `rule precedence/match-pattern/replace-pattern/` | Defines a translation rule.  
  - `precedence`: Priority of the translation rule. Range is from 1 to 15.  
  - `match-pattern`: Stream editor (SED) expression used to match incoming call information. The slash (/) is a delimiter in the pattern.  
  - `replace-pattern`: SED expression used to replace the match pattern in the call information. The slash (/) is a delimiter in the pattern. |
| **Example:**      |         |
| `Router(cfg-translation-rule)# rule 1^9//` |         |
| **Step 3**        |         |
| `exit` | Exits voice translation-rule configuration mode. |
| **Example:**      |         |
| `Router(cfg-translation-rule)# exit` |         |
| **Step 4**        |         |
| `voice translation-profile name` | Defines a translation profile for voice calls.  
  - `name`: Name of the translation profile. Maximum length of the voice translation profile name is 31 alphanumeric characters. |
| **Example:**      |         |
| `Router(config)# voice translation-profile name1` |         |
| **Step 5**        |         |
| `translate {called | calling | redirect-called} translation-rule-number` | Associates a voice translation rule with a voice translation profile.  
  - `called`: Associates the translation rule with called numbers.  
  - `calling`: Associates the translation rule with calling numbers.  
  - `redirect-called`: Associates the translation rule with redirected called numbers.  
  - `translation-rule-number`: The reference number of the translation rule from 1 to 2147483647. |
| **Example:**      |         |
| `Router(cfg-translation-profile)# translate called 1` |         |
| **Step 6**        |         |
| `exit` | Exits translation-profile configuration mode. |
| **Example:**      |         |
| `Router(cfg-translation-profile)# exit` |         |
| **Step 7**        |         |
| `call-manager-fallback` | Enters call-manager-fallback configuration mode. |
| **Example:**      |         |
| `Router(config)# call-manager-fallback` |         |
**How to Configure Cisco Unified SCCP SRST**

**Examples**

The following example shows the configuration where a translation profile called name1 is created with two voice translation rules. Rule1 consists of associated calling numbers, and rule2 consists of redirected called numbers. The Cisco Unified IP Phones in SRST mode are configured with name1.

```plaintext
voice translation-profile name1
  translate calling 1
  translate called redirect-called 2

call-manager-fallback
  translation-profile incoming name1
```

**Verifying Translation Profiles**

To verify translation profiles, perform the following steps.

**SUMMARY STEPS**

1. `show voice translation-rule number`
2. `test voice translation-rule number input-test-string [type match-type [plan match-type]]`

---

**Step 8**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **translation-profile {incoming | outgoing} name** | Assigns a translation profile for incoming or outgoing call legs on a Cisco IP phone.  
  - **incoming**: Applies the translation profile to incoming calls.  
  - **outgoing**: Applies the translation profile to outgoing calls.  
  - **name**: The name of the translation profile. |

**Example:**

```
Router(config-cm-fallback)# translation-profile outgoing name1
```

**Step 9**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>exit</strong></td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-cm-fallback)# exit
```
How to Configure Cisco Unified SCCP SRST

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>show voice translation-rule number</code></td>
<td>Use this command to verify the translation rules that you have defined for your translation profiles.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Router# show voice translation-rule 6  
Translation-rule tag: 6  
Rule 1:  
Match pattern: 65088801.  
Replace pattern: 6508880101  
Match type: none  
Replace type: none  
Match plan: none  
Replace plan: none | |

| **Step 2** | Use this command to test your translation profiles.  
See the `test voice translation-rule` command in Cisco IOS Voice Command Reference for more information. |
| `test voice translation-rule number input-test-string [type match-type [plan match-type]]` | |
| **Example:** | |
| Router(config)# voice translation-rule 5  
Router(config)# rule 1 /201/ /102/  
Router(config)# end  
Router# test voice translation-rule 5 2015550101  
Original number:2015550101  
Translated number:1025550101  
Original number type: none  
Translated number type: none  
Original number plan: none  
Translated number plan: none | |

Configuring Dial-Peer and Channel Hunting

Dial-peer hunting, the search through a group of dial peers for an available phone line, is disabled during Cisco Unified CM fallback by default. To enable dial-peer hunting, use the `no huntstop` command. For more information about dial-peer hunting, see Cisco IOS Voice Configuration Library.

If you have a dual-line phone configuration, see the “Configuring Dual-Line Phones” section on page 156. Keep incoming calls from hunting to the second channel if the first channel is busy or does not answer by using the `channel` keyword in the `huntstop` command.

Channel huntstop also prevents situations in which a call can ring for 30 seconds on the first channel of a line with no person available to answer and then ring for another 30 seconds on the second channel before rolling over to another line.

SUMMARY STEPS

1. call-manager-fallback
2. huntstop [channel]
3. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> huntstop [channel]</td>
<td>Sets the huntstop attribute for the dial peers associated with the Cisco Unified IP Phone dial peers created during Communications Manager fallback.</td>
</tr>
<tr>
<td>Example: Router(config-cm-fallback)# huntstop channel</td>
<td>• For dual-line configurations, the channel keyword keeps incoming calls from hunting to the second channel if the first channel is busy or does not answer.</td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example disables dial-peer hunting during Cisco Unified CM fallback and hunting to the secondary channels in dual-line phone configurations:

```
call-manager-fallback
no huntstop channel
```

Configuring Busy Timeout

This task sets the timeout value for call transfers to busy destinations. The busy timeout value is the amount of time that can elapse after a transferred call reaches a busy signal before the call is disconnected.

SUMMARY STEPS

1. call-manager-fallback
2. timeouts busy seconds
3. exit
DETAILLED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td>Step 2 timeouts busy seconds</td>
<td>Sets the amount of time after which calls are disconnected when they are transferred to busy destinations.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# timeouts busy 20</td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This command sets the busy timeout only for calls that are transferred to busy destinations and does not affect the timeout for calls that directly dial busy destinations.</td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example sets a timeout of 20 seconds for calls that are transferred to busy destinations:
```
call-manager-fallback
  timeouts busy 20
```

Configuring the Ringing Timeout Default

The ringing timeout default is the length of time for which a phone can ring with no answer before returning a disconnect code to the caller. This timeout prevents hung calls received over interfaces such as Foreign Exchange Office (FXO) that do not have forward-disconnect supervision. It is used only for extensions that do not have no-answer call forwarding enabled.

SUMMARY STEPS

1. call-manager-fallback
2. timeouts ringing seconds
3. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> timeouts ringing seconds</td>
<td>Sets the ringing timeout default, in seconds. The range is from 5 to 60000. There is no default value.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# timeouts ringing 30</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. `call-manager-fallback`
2. `transfer-pattern` *transfer-pattern*
3. `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></td>
</tr>
<tr>
<td><code>call-manager-fallback</code></td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# call-manager-fallback</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>transfer-pattern</code> <em>transfer-pattern</em></td>
<td>Enables the transfer of a call from a non-IP phone number to another Cisco Unified IP Phone on the same IP network using the specified transfer pattern.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-cm-fallback)# transfer-pattern 52540..</code></td>
<td>• <em>transfer-pattern</em>: String of digits for permitted call transfers. Wildcards are permitted.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-cm-fallback)# exit</code></td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
</tbody>
</table>

Examples

In the following example, the `transfer-pattern` command permits transfers from a non-IP phone number to any Cisco Unified IP Phone on the same IP network with a number in the range from 5550100 to 5550199:

`call-manager-fallback`  
`transfer-pattern 55501..`

Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0

Consultative call transfer using H.450.2 adds support for initiating call transfers and call forwarding on a call leg using the ITU-T H.450.2 and ITU-T H.450.3 standards. Call transfers and call forwarding using H.450.2 and H.450.3 can be blind or consultative. A blind call transfer or blind call forward is one in which the transferring or forwarding phone connects the caller to a destination line before a ringing tone begins. A consultative transfer is one in which the transferring or forwarding party either connects the caller to a ringing phone (ringback heard) or speaks with the third party before connecting the caller to the third party.

Note

For Cisco SRST 3.1 and later versions and Cisco Unified SRST 4.0 and later versions, call transfer and call forward using H.450.2 is supported automatically with the default session application.
Prerequisites

- Call transfer with consultation is available only when a second line or call instance is supported by the IP phone. Please see the dual-line keyword in the max-dn command.
- All voice gateway routers in the VoIP network must support the H.450 standard.
- All voice gateway routers in the VoIP network must be running the following software:
  - Cisco IOS Release 12.3(2)T or a later release
  - Cisco SRST 3.0

Restrictions

H.450.12 Supplementary Services Capabilities exchange among routers is not implemented.

SUMMARY STEPS

1. call-manager-fallback
2. call-forward pattern pattern (call forward only)
3. transfer-system {blind | full-blind | full-consult | local-consult} (call transfer only)
4. transfer-pattern transfer-pattern (call transfer only)
5. exit
6. voice service voip
7. h323
8. h450 h450-2 timeout {T1 | T2 | T3 | T4} milliseconds
9. 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>call-manager-fallback</code></td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# call-manager-fallback</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>call-forward pattern pattern</code></td>
<td>Specifies the H.450.3 standard for call forwarding.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-cm-fallback)# call-forward pattern 4...</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`transfer-system {blind</td>
<td>full-blind</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-cm-fallback)# transfer-system full-consult</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>We do not recommend the <code>blind</code> keyword. Use either the <code>full-blind</code> or <code>full-consult</code> keyword instead.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>transfer-pattern transfer-pattern</code></td>
<td>Allows transfer of telephone calls by Cisco Unified IP Phones to specified phone number patterns.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-cm-fallback)# transfer-pattern 52540..</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-cm-fallback)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Timesaver</strong></td>
<td>Before exiting call-manager-fallback configuration mode, configure any other parameters that you need to set for the entire Cisco Unified SRST phone network.</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 6</td>
<td>voice service voip</td>
<td>(Optional) Enters voice service configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> Router(config)# voice service voip</td>
</tr>
<tr>
<td>Step 7</td>
<td>h323</td>
<td>(Optional) Enters H.323 voice service configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> Router(conf-voi-serv)# h323</td>
</tr>
<tr>
<td>Step 8</td>
<td>h450 h450-2 timeout (T1</td>
<td>(Optional) Sets timeouts for supplementary service timers, in milliseconds. This command is used primarily when the default settings for these timers do not match your network delay parameters. See the ITU-T H.450.2 specification for more information on these timers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T2</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> Router(conf-serv-h323)# h450 h450-2 timeout T1 750</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>T1</strong>: Timeout value to wait to identify a response. Default is 2000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>T2</strong>: Timeout value to wait for call setup. Default is 5000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>T3</strong>: Timeout value to wait to initiate a response. Default is 5000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>T4</strong>: Timeout value to wait for setup of a response. Default is 5000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>milliseconds</strong>: Number of milliseconds. Range is from 500 to 60000.</td>
</tr>
<tr>
<td>Step 9</td>
<td>end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> Router(conf-serv-h323)# end</td>
</tr>
</tbody>
</table>

### Examples

The following example specifies transfer with consultation using the H.450.2 standard for all IP phones serviced by the Cisco Unified SRST router:

dial-peer voice 100 pots  
destination-pattern 9.T  
port 1/0/0

dial-peer voice 4000 voip  
destination-pattern 4...  
session-target ipv4:10.1.1.1

call-manager-fallback  
transfer-pattern 4...  
transfer-system full-consult

The following example enables call forwarding using the H.450.3 standard:

dial-peer voice 100 pots  
destination-pattern 9.T  
port 1/0/0
Enabling Analog Transfer Using Hookflash and the H.450.2 Standard with Cisco SRST 3.0 or Earlier

Analog call transfer using hookflash and the H.450.2 standard allows analog phones to transfer calls with consultation by using the hookflash to initiate the transfer. Hookflash refers to the short on-hook period usually generated by a telephone-like device during a call to indicate that the telephone is attempting to perform a dial-tone recall from a PBX. Hookflash is often used to perform call transfer. For example, a hookflash occurs when a caller quickly taps once on the button in the cradle of an analog phone’s handset.

This feature requires installation of a Tool Command Language (Tcl) script. The script app-h450-transfer.tcl must be downloaded from the Cisco Software Center at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp and copied to a TFTP server that is available to the Cisco Unified SRST router or copied to the flash memory on the Cisco Unified SRST router. To apply this script globally to all dial peers, use the call application global command in global configuration mode. The Tcl script has parameters to which you can pass values using attribute-value (AV) pairs in the call application voice command. The parameter that applies to this feature is as follows:

- **delay-time**: Speeds up or delays the setting up of the consultation call during a call transfer from an analog phone using a delay timer. When all digits have been collected, the delay timer is started. The call setup to the receiving party does not begin until the delay timer expires. If the transferring party goes on-hook before the delay timer expires, the transfer is considered a blind transfer rather than a consultative transfer. If the transferring party goes on-hook after the delay timer expires, either while the destination phone is ringing or after the destination party answers, the transfer is considered a consultative transfer.

In addition to the Tcl script, a ReadMe file describes the script and the configurable AV pairs. Read this file whenever you download a new version of the script because it may contain additional script-specific information, such as configuration parameters and user interface descriptions.

**Note**

For Cisco SRST 3.1 and later versions and Cisco Unified SRST 4.0 and later versions, call transfer using H.450.2 is supported automatically with the default session application.

**Prerequisites**

- The H.450 Tcl script named app-h450-transfer.tcl must be downloaded from the Cisco Software Center. The following versions of the script are available:
  - app-h450-transfer.2.0.0.2.tcl for Cisco IOS Release 12.2(11)YT1 and later releases
  - app-h450-transfer.2.0.0.1.tcl for Cisco IOS Release 12.2(11)YT
- All voice gateway routers in the VoIP network must support H.450 and be running the following software:
  - Cisco IOS Release 12.2(11)YT or a later release
  - Cisco SRST V3.0 or a lower version
- Tcl IVR 2.0
- H.450 Tcl script (app-h450-transfer.tcl)

**Note**
You can continue to use the app-h450-transfer.2.0.0.1.tcl script if you install Cisco IOS Release 12.2(11)YT1 or later, but you cannot use the app-h450-transfer.2.0.0.2.tcl script with a release of Cisco IOS software that is earlier than Cisco IOS Release 12.2(11)YT1.

**Restrictions**

- When a consultative transfer is made by an analog FXS phone using hookflash, the consultation call itself cannot be further transferred (that is, it cannot become a recursive or chained transfer) until after the initial transfer operation is completed and the transferee and transfer-to parties are connected. After the initial call transfer operation is completed and the transferee and transfer-to parties are now the only parties in the call, the transfer-to party may further transfer the call.
- Call transfer with consultation is not supported for Cisco ATA-186, Cisco ATA-188, and Cisco IP Conference Station 7935. Transfer attempts from these devices are executed as blind transfers.

**SUMMARY STEPS**

1. call application voice application-name location
2. call application voice application-name language number language
3. call application voice application-name set-location language category location
4. call application voice application-name delay-time seconds
5. dial-peer voice number pots
6. application application-name
7. exit
8. dial-peer voice number voip
9. application application-name
10. exit


<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** call application voice application-name location | Loads the Tcl script and specifies its application name.  
  - *application-name*: User-defined name for the IVR application. This name does not have to match the script filename.  
  - *location*: Script directory and filename in URL format. For example, flash memory (flash:filename), a TFTP (tftp://..filename), or an HTTP server (http://..filename) are valid locations. |
| Example: Router(config)# call application voice transfer_app flash:app-h450-transfer.tcl | |
| **Step 2** call application voice application-name language number language | (Optional) Sets the language for dynamic prompts used by the application.  
  - *application-name*: IVR application name that was assigned in Step 1.  
  - *number*: Number that identifies the language used by the audio files for the IVR application.  
  - *language*: Two-character code that specifies the language of the prompts. Valid entries are *en* (English: default), *sp* (Spanish), *ch* (Chinese), or *aa* (all). |
| Example: Router(config)# call application voice transfer_app language 1 en | |
| **Step 3** call application voice application-name set-location language category location | Defines the location and category of the audio files that are used by the application for dynamic prompts.  
  - *application-name*: Name of the Tcl IVR application.  
  - *language*: Two-character code to specify the language of the prompts. Valid entries are *en* (English: default), *sp* (Spanish), *ch* (Chinese), or *aa* (all).  
  - *category*: Category group (0 to 4) for the audio files from this location. The value 0 means all categories.  
  - *location*: URL of the directory that contains the language audio files used by the application, without filenames. Flash memory (flash) or a directory on a server (TFTP, HTTP, or RTSP) are all valid. |
| Example: Router(config)# call application voice transfer_app set-location en 0 flash:/prompts | Prompts are required for call transfer from analog FXS phones. No prompts are needed for call transfer from IP phones. |
### Command or Action

#### Step 4
```
call application voice application-name delay-time seconds
```
*(Optional) Sets the delay time for consultation call setup for an analog phone that is making a call transfer using the H.450 application. This command passes a value to the Tcl script by using an attribute-value (AV) pair.

- **seconds**: Number of seconds to delay call setup. Range is from 1 to 10. Default is 2.

A delay of more than 2 seconds is generally noticeable to users.

For more information about AV pairs and the Tcl script for H.450 call transfer and forwarding, see the ReadMe file that accompanies the script.

#### Example:
```
Router(config)# call application voice transfer_app delay-time 1
```

#### Step 5
```
dial-peer voice number pots
```
Enters dial-peer configuration mode to configure a POTS dial peer.

#### Example:
```
Router(config)# dial-peer voice 25 pots
```

#### Step 6
```
application application-name
```
Loads the application named in Step 1 onto the dial peer.

#### Example:
```
Router(config-dial-peer)# application transfer_app
```

#### Step 7
```
exit
```
Exits dial-peer configuration mode.

#### Example:
```
Router(config-dial-peer)# exit
```

#### Timesaver
Before exiting dial-peer configuration mode, configure any other dial-peer parameters that you need to set for this dial peer.

#### Step 8
```
dial-peer voice number voip
```
Enters dial-peer configuration mode to configure a VoIP dial peer.

#### Example:
```
Router(config)# dial-peer voice 29 voip
```

#### Step 9
```
application application-name
```
Loads the application named in Step 1 onto the dial peer.

#### Example:
```
Router(config-dial-peer)# application transfer_app
```

#### Step 10
```
exit
```
Exits dial-peer configuration mode.

#### Example:
```
Router(config-dial-peer)# exit
```

#### Timesaver
Before exiting dial-peer configuration mode, configure any other dial-peer parameters that you need to set for this dial peer.
Examples

The following example enables the H.450 Tcl script for analog transfer using hookflash and sets a delay time of 1 second:

call application voice transfer_app flash:app-h450-transfer.tcl
call application voice transfer_app language 1 en
call application voice transfer_app set-location en 0 flash:/prompts
call application voice transfer_app delay-time 1
!
dial-peer voice 25 pots
destination-pattern 9.T
port 1/0/0
application transfer_app
!
dial-peer voice 29 voip
destination-pattern 4_
session-target ipv4:10.1.10.1
application transfer_app

Configuring Trunk Access Codes

Note Configure trunk access codes only if your normal network dial-plan configuration prevents you from configuring permanent POTS voice dial peers to provide trunk access for use during fallback. If you already have local PSTN ports configured with the appropriate access codes provided by dial peers (for example, dial 9 to select an FXO PSTN line), this configuration is not needed.

Trunk access codes provide IP phones with access to the PSTN during Cisco Unified CM fallback by creating POTS voice dial peers that are active during Cisco Unified CM fallback only. These temporary dial peers, which can be matched to voice ports (BRI, E&M, FXO, and PRI), allow Cisco Unified IP Phones access to trunk lines during Cisco Unified CM mode. When Cisco Unified SRST is active, all PSTN interfaces of the same type are treated as equivalent, and any port may be selected to place the outgoing PSTN call.

Trunk access codes are created using the access-code command.

SUMMARY STEPS

1. call-manager-fallback
2. access-code \{\{fxo | e&m\} dial-string | \{bri | pri\} dial-string [direct-inward-dial]\} 
3. exit
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> access-code {fxo</td>
<td>e&amp;m} dial-string</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# access-code e&amp;m 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example creates access code number 8 for BRI and enables DID on the POTS dial peer:

```
call-manager-fallback
access-code bri 8 direct-inward-dial
```

**Configuring Interdigit Timeout Values**

Configuring interdigit timeout values involves specifying how long, in seconds, all Cisco Unified IP Phones attached to a Cisco Unified SRST router are to wait after an initial digit or a subsequent digit is dialed. The **timeouts interdigit** timer is enabled when a caller enters a digit and is restarted each time the caller enters subsequent digits until the destination address is identified. If the configured timeout value is exceeded before the destination address is identified, a tone sounds and the call is terminated.
SUMMARY STEPS

1. call-manager-fallback
2. timeouts interdigit seconds
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td>(Optional) Configures the interdigit timeout value for all Cisco IP phones that are attached to the router.</td>
</tr>
<tr>
<td>Step 2 timeouts interdigit seconds</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# timeouts interdigit 5</td>
<td>seconds: Interdigit timeout duration, in seconds, for all Cisco Unified IP Phones. Valid entries are integers from 2 to 120.</td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example sets the interdigit timeout value to 5 seconds for all Cisco Unified IP Phones. In this example, 5 seconds are the elapsed time after which an incompletely dialed number times out. For example, a caller who dials nine digits (408555010) instead of the required ten digits (4085550100) will hear a busy tone after the second timeout elapses.

call-manager-fallback
timeouts interdigit 5

Configuring Class of Restriction

The class of restriction (COR) functionality provides the ability to deny certain call attempts on the basis of the incoming and outgoing class of restrictions provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, calls to 900 numbers), and applies different restrictions to call attempts from different originators. The `cor` command sets the dial-peer COR parameter for dial peers associated with the directory numbers created during Communications Manager fallback.

You can have up to 20 COR lists for each incoming and outgoing call. A default COR is assigned to directory numbers that do not match any COR list numbers or number ranges. An assigned COR is invoked for the dial peers and created for each directory number automatically during Communications Manager fallback registration.

If a COR is applied on an incoming dial peer (for incoming calls) and it is a superset of or is equal to the COR applied to the outgoing dial peer (for outgoing calls), the call will go through. Voice ports determine whether a call is considered incoming or outgoing. If you hook up a phone to an FXS port on
a Cisco Unified SRST router and try to make a call from that phone, the call will be considered an incoming call to the router and voice port. If you make a call to the FXS phone, the call will be considered outgoing.

By default, an incoming call leg has the highest COR priority; the outgoing call leg has the lowest priority. If there is no COR configuration for incoming calls on a dial peer, you can make a call from a phone attached to the dial peer, so that the call will go out of any dial peer regardless of the COR configuration on that dial peer. Table 8-2 describes call functionality based on how your COR lists are configured.

Table 8-2 Combinations of COR List and Results

<table>
<thead>
<tr>
<th>COR List on Incoming Dial Peer</th>
<th>COR List on Outgoing Dial Peer</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>No COR</td>
<td>No COR</td>
<td>Call will succeed.</td>
</tr>
<tr>
<td>No COR</td>
<td>COR list applied for outgoing calls</td>
<td>Call will succeed. By default, the incoming dial peer has the highest COR priority when no COR is applied. If you apply no COR for an incoming call leg to a dial peer, the dial peer can make a call out of any other dial peer regardless of the COR configuration on the outgoing dial peer.</td>
</tr>
<tr>
<td>COR list applied for incoming calls</td>
<td>No COR</td>
<td>Call will succeed. By default, the outgoing dial peer has the lowest priority. Because there are some COR configurations for incoming calls on the incoming or originating dial peer, it is a superset of the outgoing call’s COR configuration for the outgoing or terminating dial peer.</td>
</tr>
<tr>
<td>COR list applied for incoming calls (superset of COR list applied for outgoing calls on the outgoing dial peer)</td>
<td>COR list applied for outgoing calls (subsets of COR list applied for incoming calls on the incoming dial peer)</td>
<td>Call will succeed. The COR list for incoming calls on the incoming dial peer is a superset of the COR list for outgoing calls on the outgoing dial peer.</td>
</tr>
<tr>
<td>COR list applied for incoming calls (subset of COR list applied for outgoing calls on the outgoing dial peer)</td>
<td>COR list applied for outgoing calls (supersets of COR list applied for incoming calls on the incoming dial peer)</td>
<td>Call will not succeed. The COR list for incoming calls on the incoming dial peer is not a superset of the COR list for outgoing calls on the outgoing dial peer.</td>
</tr>
</tbody>
</table>

SUMMARY STEPS

1. call-manager-fallback
2. cor {incoming | outgoing} cor-list-name {cor-list-number starting-number - ending-number | default}
3. 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>call-manager-fallback</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# call-manager-fallback</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>cor</strong> (incoming</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# cor outgoing LockforPhoneC 1 5010 – 5020</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-cm-fallback)# exit</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to set a dial-peer COR parameter for outgoing calls to the Cisco Unified IP Phone dial peers and directory numbers created during fallback:

```
call-manager-fallback
cor outgoing LockforPhoneC 1 5010 – 5020
```

The following example shows how to set the dial-peer COR parameter for incoming calls to the Cisco IP phone dial peers and directory numbers in the default COR list:

```
call-manager-fallback
cor incoming LockforPhoneC default
```

The following example shows how sub- and super-COR sets are created. First, a custom dial-peer COR is created with names declared under it:

```
dial-peer cor custom
   name 911
   name 1800
   name 1900
   name local_call
```
In the following configuration example, COR lists are created and applied to the dial peer:

dial-peer cor list call911
   member 911

dial-peer cor list call1800
   member 1800

dial-peer cor list call1900
   member 1900

dial-peer cor list calllocal
   member calllocal

In the example below, five dial peers are configured for destination numbers 734...., 1800...., 1900...., 316...., and 911. A COR list is applied to each of the dial peers.

dial-peer voice 1 voip
   destination pattern 734....
   session target ipv4:10.1.1.1
   cor outgoing calllocal

In the example below, five dial peers are configured for destination numbers 1800...., 1900...., 316...., and 911. A COR list is applied to each of the dial peers.

dial-peer voice 1 voip
   destination pattern 734....
   session target ipv4:10.1.1.1
   cor outgoing calllocal

dial-peer voice 2 voip
   destination pattern 1800....
   session target ipv4:10.1.1.1
   cor outgoing call1800

Finally, the COR list is applied to the individual phone numbers.

call-manager-fallback
   max-conferences 8
   cor incoming engineering 1 1001 - 1001
   cor incoming hr 2 1002 - 1002
   cor incoming manager 3 1003 - 1008
The sample configuration allows for the following:

- Extension 1001 to call 734... numbers, 911, and 316....
- Extension 1002 to call 734..., 1800 numbers, 911, and 316....
- Extension 1003 to 1008 to call all of the possible Cisco Unified SRST router numbers
- All extensions to call 316....

**Call Blocking (Toll Bar) Based on Time of Day and Day of Week or Date**

Call blocking to prevent unauthorized use of phones is implemented by matching a pattern of specified digits during a specified time of day and day of week or date. Up to 32 patterns of digits can be specified. Call blocking is supported on IP phones only and not on analog foreign exchange station (FXS) phones.

When a user attempts to place a call to digits that match a pattern that is specified for call blocking during a time period that is defined for call blocking, a fast busy signal is played for approximately 10 seconds. The call is then terminated, and the line is placed back in on-hook status.

In SRST (call-manager-fallback configuration) mode, there is no phone- or pin-based exemption to after-hours call blocking.

**SUMMARY STEPS**

1. call-manager-fallback
2. after-hours block pattern tag pattern [7-24]
3. after-hours day day start-time stop-time
4. after-hours date month date start-time stop-time
5. exit
### How to Configure Cisco Unified SCCP SRST

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>call-manager-fallback</code></td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# call-manager-fallback</code></td>
<td>Defines a pattern of outgoing digits to be blocked. Up to 32 patterns can be defined, using individual commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If the 7-24 keyword is specified, the pattern is always blocked, 7 days a week, 24 hours a day.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If the 7-24 keyword is not specified, the pattern is blocked during the days and dates that are defined using the <code>after-hours day</code> and <code>after-hours date</code> commands.</td>
</tr>
<tr>
<td>2</td>
<td><code>after-hours block pattern [7-24]</code></td>
<td>Defines a recurring time period based on the day of the week during which calls are blocked to outgoing dial patterns that are defined using the <code>after-hours block pattern</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-cm-fallback)# after-hours block pattern 1 91900</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>after-hours day day start-time stop-time</code></td>
<td>Defines a recurring time period based on month and date during which calls are blocked to outgoing dial patterns that are defined using the <code>after-hours block pattern</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-cm-fallback)# after-hours day mon 19:00 7:00</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>after-hours date month date start-time stop-time</code></td>
<td>Defines a recurring time period based on month and date during which calls are blocked to outgoing dial patterns that are defined using the <code>after-hours block pattern</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-cm-fallback)# after-hours date jan 1 0:00 0:00</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>exit</code></td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-cm-fallback)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

### Examples

- `Router(config)# call-manager-fallback`  
- `Router(config-cm-fallback)# after-hours block pattern 1 91900`  
- `Router(config-cm-fallback)# after-hours day mon 19:00 7:00`  
- `Router(config-cm-fallback)# after-hours date jan 1 0:00 0:00`  
- `Router(config-cm-fallback)# exit`
The following example defines several patterns of digits for which outgoing calls are blocked. Patterns 1 and 2, which block calls to external numbers that begin with “1” and “011,” are blocked on Monday through Friday before 7 a.m. and after 7 p.m., on Saturday before 7 a.m. and after 1 p.m., and all day Sunday. Pattern 3 blocks calls to 900 numbers 7 days a week, 24 hours a day.

call-manager-fallback
after-hours block pattern 1 91
after-hours block pattern 2 9011
after-hours block pattern 3 91900 7-24
after-hours block day mon 19:00 07:00
after-hours block day tue 19:00 07:00
after-hours block day wed 19:00 07:00
after-hours block day thu 19:00 07:00
after-hours block day fri 19:00 07:00
after-hours block day sat 13:00 12:00
after-hours block day sun 12:00 07:00

How to Configure Cisco Unified SIP SRST

This section contains the following procedures:

- Configuring SIP Phone Features, page 224 (optional)
- Configuring SIP-to-SIP Call Forwarding, page 226 (required)
- Configuring Call Blocking Based on Time of Day, Day of Week, or Date, page 228 (required)
- SIP Call Hold and Resume, page 228 (no configuration necessary)
- Examples, page 232

Configuring SIP Phone Features

After a voice register pool has been set, this procedure adds optional features to increase functionality. Some features can be made per pool or globally.

In voice register pool configuration, you can now configure several new options per pool (a pool can be one phone or a group of phones). There is also a new voice register global configuration mode for Cisco Unified SIP SRST. In voice register global mode, you can globally assign characteristics to phones.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register global tag
4. max-pool max-voice-register-pools
5. application application-name
6. external ring {bellcore-dr1 | bellcore-dr2 | bellcore-dr3 | bellcore-dr4 | bellcore-dr5}
7. exit
8. voice register pool tag
9. no vad
10. `codec codec-type [bytes]`

11. `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 register global tag` | Enters voice register global configuration mode to set global parameters for all supported Cisco SIP IP phones in a Cisco Unified SIP SRST environment. |
| Example: `Router(config)# voice register global 12` | |
| **Step 4** `max-pool max-voice-register-pools` | Sets the maximum number of SIP voice register pools that are supported in a Cisco Unified SIP SRST environment.  
* The `max-voice-register-pools` argument represents the maximum number of SIP voice register pools supported by the Cisco Unified SIP SRST router. The upper limit of voice register pools is version- and platform-dependent; see Cisco IOS command-line interface (CLI) help. Default is 0. |
| Example: `Router(config-register-global)# max-pool 10` | |
| **Step 5** `application application-name` | Selects the session-level application for all dial peers associated with SIP phones. Use the `application-name` argument to define a specific interactive voice response (IVR) application. |
| Example: `Router(config-register-global)# application global_app` | |
| **Step 6** `external-ring (bellcore-dr1 | bellcore-dr2 | bellcore-dr3 | bellcore-dr4 | bellcore-dr5)` | Specifies the type of ring sound used on Cisco SIP or Cisco SCCP IP phones for external calls. Each `bellcore-dr` 1-5 keyword supports standard distinctive ringing patterns as defined in the standard GR-506-CORE, *LSSGR: Signaling for Analog Interfaces*. |
| Example: `Router(config-register-global)# external-ring bellcore-dr1` | |
| **Step 7** `exit` | Exits voice register global configuration mode. |
| Example: `Router(config-register-global)# exit` | |
| **Step 8** `voice register pool tag` | Enters voice register pool configuration mode for SIP phones.  
* Use this command to control which phone registrations are to be accepted or rejected by a Cisco Unified SIP SRST device. |
| Example: `Router(config)# voice register pool 20` | |
Configuring SIP-to-SIP Call Forwarding

SIP-to-SIP call forwarding (call routing) is available. Call forwarding is provided either by the phone or by using a back-to-back user agent (B2BUA), which allows call forwarding on any dial peer. Calls into a SIP device may be forwarded to other SIP or SCCP devices (including Cisco Unity, third-party voice-mail systems, or an auto attendant or IVR system such as IPCC and IPCC Express). In addition, SCCP IP phones may be forwarded to SIP phones. Cisco Unity or other voice messaging systems connected by a SIP trunk or SIP user agent are able to pass a message-waiting indicator (MWI) when a message is left. The SIP phone then displays the MWI when indicated by the voice messaging system.

Note

SIP-to-H.323 call forwarding is not supported.

To configure SIP-to-SIP call forwarding, you must first allow connections between specific types of endpoints in a Cisco IP-to-IP gateway. The **allow-connections** command grants this capability. Once the SIP-to-SIP connections are allowed, you can configure call forwarding under an individual SIP phone pool. Any of the following commands can be used to configure call forwarding, according to your needs:

- **Under voice register pool**
  - `call-forward b2bua all directory-number`
  - `call-forward b2bua busy directory-number`
  - `call-forward b2bua mailbox directory-number`
  - `call-forward b2bua noan directory-number [timeout seconds]`
In a typical Cisco Unified SIP SRST setup, the call-forward b2bua mailbox command is not used; however, it is likely to be used in a Cisco Unified SIP Communications Manager Express (CME) environment. Detailed procedures for configuring the call-forward b2bua mailbox command are found in the Cisco Unified Communications Manager (CallManager) documentation on Cisco.com.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice register pool tag
4. call-forward b2bua all directory-number
5. call-forward b2bua busy directory-number
6. call-forward b2bua mailbox directory-number
7. call-forward b2bua noan directory-number timeout seconds
8. 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>• 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>Enters voice register pool configuration mode.</td>
</tr>
<tr>
<td>Step 3 voice register pool tag</td>
<td>• Use this command to control which phone registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters voice register pool configuration mode.</td>
</tr>
<tr>
<td>Step 4 call-forward b2bua all</td>
<td>Enables call forwarding for a SIP back-to-back user agent (B2BUA) so that all incoming calls are forwarded to another non-SIP station extension (that is, SIP trunk, H.323 trunk, SCCP device or analog/digital trunk).</td>
</tr>
<tr>
<td>directory-number</td>
<td>• directory-number: Telephone number to which calls are forwarded. Represents a fully qualified E.164 number. Maximum length of the telephone number is 32.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-pool)# call-forward b2bua all 5005</td>
</tr>
<tr>
<td>Step 5 call-forward b2bua busy</td>
<td>Enables call forwarding for a SIP B2BUA so that incoming calls to a busy extension are forwarded to another extension.</td>
</tr>
<tr>
<td>directory-number</td>
<td>• directory-number: Telephone number to which calls are forwarded. Represents a fully qualified E.164 number. Maximum length of the telephone number is 32.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-pool)# call-forward b2bua busy 5006</td>
</tr>
</tbody>
</table>
How to Configure Cisco Unified SIP SRST

Configuring Call Blocking Based on Time of Day, Day of Week, or Date

This section applies to both SCCP and SIP SRST. Call blocking prevents the unauthorized use of phones and is implemented by matching a pattern of up to 32 digits during a specified time of day, day of week, or date. Cisco Unified SIP SRST provides SIP endpoints the same time-based call blocking mechanism that is currently provided for SCCP phones. The call blocking feature supports all incoming calls, including incoming SIP and analog FXS calls.

Note
Pin-based exemptions and the “Login” toll-bar override are not supported in Cisco Unified SIP SRST.

The commands used for SIP phone call blocking are the same commands that are used for SCCP phones on your Cisco Unified SRST system. The Cisco SRST session application accesses the current after-hours configuration under call-manager-fallback mode and applies it to calls originated by Cisco SIP phones that are registered to the Cisco SRST router. The commands used in call-manager-fallback mode that set block criteria (time/date/block pattern) are the following:

- **after-hours block pattern** pattern-tag pattern [7-24]
- **after-hours day** day start-time stop-time
- **after-hours date** month date start-time stop-time

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6&lt;br&gt;call-forward b2bua mailbox directory-number</td>
<td>Controls the specific voice-mail box selected in a voice-mail system at the end of a call forwarding exchange.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;Router(config-register-pool)# call-forward b2bua mailbox 5007</td>
<td></td>
</tr>
<tr>
<td>Step 7&lt;br&gt;call-forward b2bua noan directory-number timeout seconds</td>
<td>Enables call forwarding for a SIP B2BUA so that incoming calls to an extension that does not answer after a configured amount of time are forwarded to another extension.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;Router(config-register-pool)# call-forward b2bua noan 5010 timeout 10</td>
<td></td>
</tr>
<tr>
<td>Step 8&lt;br&gt;end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:&lt;br&gt;Router(config-register-pool)# end</td>
<td></td>
</tr>
</tbody>
</table>
When a user attempts to place a call to digits that match a pattern that has been specified for call blocking during a time period that has been defined for call blocking, the call is immediately terminated and the caller hears a fast busy.

In SRST (call-manager-fallback configuration mode), there is no phone- or pin-based exemption to after-hours call blocking. However, in Cisco Unified SIP SRST (voice register pool mode), individual IP phones can be exempted from all call blocking using the `after-hours exempt` command.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `after-hours block pattern tag pattern [7-24]`
5. `after-hours day day start-time stop-time`
6. `after-hours date month date start-time stop-time`
7. `exit`
8. `voice register pool tag`
9. `after-hour exempt`
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.  
  • Enter your password if prompted. |
| **Example:**  
  Router> enable | |
| **Step 2** `configure terminal` | Enters global configuration mode. |
| **Example:**  
  Router# configure terminal | |
| **Step 3** `call-manager-fallback` | Enters call-manager-fallback configuration mode. |
| **Example:**  
  Router(config)# call-manager-fallback | |
| **Step 4** `after-hours block pattern tag pattern [7-24]` | Defines a pattern of outgoing digits to be blocked. Up to 32 patterns can be defined, using individual commands.  
  • If the 7-24 keyword is specified, the pattern is always blocked, 7 days a week, 24 hours a day.  
  • If the 7-24 keyword is not specified, the pattern is blocked during the days and dates that are defined using the `after-hours day` and `after-hours date` commands. |
| **Example:**  
  Router(config-cm-fallback)# after-hours block pattern 1 91900 | |
### Command or Action

#### Step 5

`after-hours day start-time stop-time`

**Example:**

Router(config-cm-fallback)# after-hours day mon 19:00 07:00

**Purpose:** Defines a recurring time period based on the day of the week during which calls are blocked to outgoing dial patterns that are defined using the `after-hours block pattern` command.

- **day:** Day of the week abbreviation. The following are valid day abbreviations: sun, mon, tue, wed, thu, fri, sat.
- **start-time stop-time:** Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs on the day following the start time. For example, “mon 19:00 07:00” means “from Monday at 7 p.m. until Tuesday at 7 a.m.”

The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.

#### Step 6

`after-hours date month date start-time stop-time`

**Example:**

Router(config-cm-fallback)# after-hours date jan 1 00:00 00:00

**Purpose:** Defines a recurring time period based on month and date during which calls are blocked to outgoing dial patterns that are defined using the `after-hours block pattern` command.

- **month:** Month abbreviation. The following are valid month abbreviations: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec.
- **date:** Date of the month. Range is from 1 to 31.
- **start-time stop-time:** Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. The stop time must be larger than the start time.

The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.

#### Step 7

`exit`

**Example:**

Router(config-cm-fallback)# exit

**Purpose:** Exits call-manager-fallback configuration mode.

#### Step 8

`voice register pool tag`

**Example:**

Router(config)# voice register pool 12

**Purpose:** Enters voice register pool configuration mode.

- **Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device.**
### Examples

The following example defines several patterns of digits for which outgoing calls are blocked. Patterns 1 and 2, which block calls to external numbers that begin with 1 and 011, are blocked on Monday through Friday before 7 a.m. and after 7 p.m. Pattern 3 blocks calls to 900 numbers 7 days a week, 24 hours a day.

```plaintext
call-manager-fallback
after-hours block pattern 1 91
after-hours block pattern 2 9011
after-hours block pattern 3 91900 7-24
after-hours day mon 19:00 07:00
after-hours day tue 19:00 07:00
after-hours day wed 19:00 07:00
after-hours day thu 19:00 07:00
after-hours day fri 19:00 07:00
```

The following example exempts a Cisco SIP phone pool from the configured blocking criteria:

```plaintext
voice register pool 1
after-hour exempt
```

### Verification

To verify the feature’s configuration, enter one of the following commands:

- **show voice register dial-peer**: Displays all the dial peers created dynamically by phones that have registered. This command also displays configurations for after hours blocking and call forwarding.
- **show voice register pool <tag>**: Displays information regarding a specific pool.
- **debug ccsip message**: Debugs basic B2BUA calls.

For more information about these commands, see *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions).*
SIP Call Hold and Resume

Cisco Unified SRST supports the ability for SIP phones to place calls on hold and to resume from calls placed on hold. This also includes support for a consultative hold where A calls B, B places A on hold, B calls C, and B disconnects from C and then resumes with A. Support for call hold is signaled by SIP phones using “re-INVITE c=0.0.0.0” and also by the receive-only mechanism.

No configuration is necessary.

Examples

Router# show running-config
Building configuration...

Current configuration : 1462 bytes
configuration mode exclusive manual
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
boot-start-marker
boot-end-marker
!
logging buffered 8000000 debugging
!
no aaa new-model
!
resource policy
!
clock timezone edt -5
clock summer-time edt recurring
ip subnet-zero
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
id mac 0012.7F57.60AA
number 1 1000
call-forward b2bua busy 2413
call-forward b2bua noan 2414 timeout 30

codec g711ulaw
!

voice register pool 2
id mac 0012.7F3B.9025
number 1 2800
codec g711ulaw
!

voice register pool 3
id mac 0012.7F57.628F
number 1 2801
codec g711ulaw
!
!

interface GigabitEthernet0/0
ip address 10.0.2.99 255.255.255.0
duplex auto
speed auto
!

interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip http server
!
!
control-plane
!
!

dial-peer voice 1000 voip
destination-pattern 24..
session protocol sipv2
session target ipv4:10.0.2.5
codec g711ulaw
!
! Define call blocking under call-manager-fallback mode

call-manager-fallback
max-conferences 4 gain -6
after-hours block pattern 1 2417

after-hours date Dec 25 12:01 20:00
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
How to Configure Optional Features

This section describe the following optional additional call features:

- Three-party G.711 ad hoc conferencing—Cisco Unified Survivable Remote Site Telephony (SRST) support for simultaneous three-party conferences.
- eXtensible Markup Language (XML) application program interface (API)—This interface supplies data from Cisco Unified SRST to management software.

The following sections describe how to configure these optional features:

- Enabling Three-Party G.711 Ad Hoc Conferencing, page 234
- Defining XML API Schema, page 236

Enabling Three-Party G.711 Ad Hoc Conferencing

Enabling three-party G.711 ad hoc conferencing involves configuring the maximum number of simultaneous three-party conferences supported by the Cisco Unified SRST router. For conferencing to be available, an IP phone must have a minimum of two lines connected to one or more buttons. See the “Configuring a Secondary Dial Tone” section on page 155.

SUMMARY STEPS

1. call-manager-fallback
2. max-conferences max-conference-numbers
3. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  call-manager-fallback | Enters call-manager-fallback configuration mode. |
| **Example:**
  Router(config)# call-manager-fallback | |
| **Step 2**
  max-conferences max-conference-numbers | Sets the maximum number of simultaneous three-party conferences supported by the router. The maximum number possible is platform dependent: |
  • Cisco 1751 router:8
  • Cisco 1760 router:8
  • Cisco 2600 series routers:8
  • Cisco 2600-XM series routers:8
  • Cisco 2801 router:8
  • Cisco 2811, Cisco 2821, and Cisco 2851 routers:16
  • Cisco 3640 and Cisco 3640A routers:8
  • Cisco 3660 router:16
  • Cisco 3725 router:16
  • Cisco 3745 router:16
  • Cisco 3800 series router:24 |
| **Example:**
  Router(config-cm-fallback)# max-conferences 16 | |
| **Step 3**
  exit | Exits call-manager-fallback configuration mode. |
| **Example:**
  Router(config-cm-fallback)# exit | |

Examples

The following example configures up to eight simultaneous three-way conferences on a router:

```
call-manager-fallback
max-conferences 8
```
Defining XML API Schema

The Cisco IOS commands in this section allow you to specify parameters associated with the XML API. For more information, see XML Provisioning Guide for Cisco CME/SRST. See the “Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0” section on page 208 for configuration instructions.

SUMMARY STEPS

1. call-manager-fallback
2. xmlschema schema-url
3. 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 call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# call-manager-fallback</td>
</tr>
</tbody>
</table>

| **Step 2** | Specifies the URL for an XML API schema to be used with this Cisco Unified SRST system. |
| xmlschema schema-url | |
| **Example:** | Router(config-cm-fallback)# xmlschema http://server2.example.com/schema/schemal.xsd |
| *schema-url:* Local or remote URL as defined in RFC 2396. |

| **Step 3** | Exits call-manager-fallback configuration mode. |
| exit | |
| **Example:** | Router(config-cm-fallback)# exit |

Configuration Examples for Call Handling

- Example: Monitoring the Status of Key Expansion Modules, page 236
- Example: Configuring Voice Hunt Groups in Cisco Unified SIP SRST, page 237

Example: Monitoring the Status of Key Expansion Modules

Show commands are used to monitor the status and other details of Key Expansion Modules (KEMs). The following example demonstrates how the `show voice register all` command displays KEM details with all the Cisco Unified CME configurations and registration information:

```
show voice register all
VOICE REGISTER GLOBAL
========================
CONFIG [Version=9.1]
```
Pool Tag 5
Config:
  Mac address is B4A4.E328.4698
  Type is 9971 addon 1 CKEM
  Number list 1 : DN 2
  Number list 2 : DN 3
  Proxy Ip address is 0.0.0.0
  DTMF Relay is disabled
  Call Waiting is enabled
  DnD is disabled
  Video is enabled
  Camera is enabled
  Busy trigger per button value is 0
  keep-conference is enabled
  registration expires timer max is 200 and min is 60
  kpml signal is enabled
  Lpcor Type is none

The following example demonstrates how the `show voice register pool type` command displays all the phones configured with add-on KEMs in Cisco Unified CME:

```plaintext
Router# show voice register pool type CKEM
Pool ID  IP Address     Ln DN  Number   State
==== ============== =============== === =========== ===========
 4   B4A4.E328.4698  9.45.31.111     1  4   5589$     REGISTERED
```

Example: Configuring Voice Hunt Groups in Cisco Unified SIP SRST

The following example shows how to configure longest-idle hunt group 20 with pilot number 4701, final number 5000, and 6 numbers in the list. After a call is redirected six times (makes 6 hops), it is redirected to the final number 5000.

```plaintext
Router(config)# voice hunt-group 20 longest-idle
Router(config-voice-hunt-group)# pilot 4701
Router(config-voice-hunt-group)# list 4001, 4002, 4023, 4028, 4045, 4062
Router(config-voice-hunt-group)# final 5000
Router(config-voice-hunt-group)# hops 6
Router(config-voice-hunt-group)# timeout 20
Router(config-voice-hunt-group)# exit
```

Where to Go Next

If you need to configure security, see the “Configuring Secure SRST for SCCP and SIP” section on page 239, or if you need to configure voicemail, see the “Integrating Voicemail with Cisco Unified SRST” section on page 331. If you need to configure video parameters, see the “Setting Video Parameters” section on page 355. If you do not need any of those features, go to the “Monitoring and Maintaining Cisco Unified SRST” section on page 369.

For additional information, see the “Additional References” section on page 308 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
Configuring Secure SRST for SCCP and SIP

The Secure SRST adds security functionality to the Unified SRST.

Note
Unified Secure SRST 12.6 on Cisco IOS XE Gibraltar 16.11.1a Release is not a recommended release version for Unified Secure SCCP SRST call flows and call flows that include stcapp configuration.

Contents
This chapter describes new Secure SRST security features such as authentication, integrity, and media encryption.

- Prerequisites for Configuring Secure SRST, page 239
- Restrictions for Configuring Secure SRST, page 240
- Information About Configuring Secure SRST, page 242
- How to Configure Secure Unified SRST, page 254
- Additional References, page 308
- Command Reference, page 310
- Feature Information for Secure SCCP and SIP SRST, page 311
- Where to Go Next, page 311

Prerequisites for Configuring Secure SRST

General
- Secure Cisco Unified IP phones supported in secure SCCP and SIP SRST must have the Certification Authority (CA) or third-party certificates installed, and encryption enabled. For more information on CA server authentication, see Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 257.
- The SRST router must have a certificate; a certificate can be generated by a third party or by the Cisco IOS certificate authority (CA). The Cisco IOS CA can run on the same gateway as Cisco Unified SRST. Over the TLS channel (port 2445), automated certificate exchange happens between
the Unified SRST router and the Cisco Unified Communications Manager. However, the phone certificate exchange to Unified SRST through Unified Communications Manager has to be downloaded manually on the Unified SRST router.

- Certificate trust lists (CTLs) on Cisco Unified Communications Manager must be enabled.
- It is mandatory to configure the command `supplementary-service media-renegotiate` under `voice service voip` configuration mode to enable the supplementary features supported on Unified Secure SRST.

### Public Key Infrastructure on Secure SRST
- Set the clock, either manually or by using Network Time Protocol (NTP). Setting the clock ensures synchronicity with Cisco Unified Communications Manager.
- Enable the IP HTTP server (Cisco IOS processor) with the `ip http server` command, if not already enabled. For more information on public key infrastructure (PKI) deployment, see the Cisco IOS Certificate Server feature.
- If the certificate server is part of your startup configuration, you may see the following messages during the boot procedure:
  ```
  % Failed to find Certificate Server's trustpoint at startup
  % Failed to find Certificate Server's cert.
  ```

  These messages are informational messages and indicate a temporary inability to configure the certificate server because the startup configuration has not been fully parsed yet. The messages are useful for debugging, in case the startup configuration is corrupted.

  You can verify the status of the certificate server after the boot procedure using the `show crypto pki server` command.

### Supported Cisco Unified IP Phones, Platforms, and Memory Requirements
- For a list of supported Cisco Unified IP Phones, routers, network modules, and codecs for secure SRST, see the Cisco Unified Survivable Remote Site Telephony Compatibility Information feature.
- For the most up-to-date information about the maximum number of Cisco Unified IP Phones, the maximum number of directory numbers (DNs) or virtual voice ports, and memory requirements, see the Cisco Unified SRST 12.3 Supported Firmware, Platforms, Memory, and Voice Products feature.

## Restrictions for Configuring Secure SRST

### General
- Cryptographic software features ("k9") are under export controls. This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and, users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

  A summary of U.S. laws governing Cisco cryptographic products may be found at the following URL:

  If you require further assistance, please contact us by sending email to export@cisco.com.
Restrictions for Configuring Secure SRST

When a Secure Real-Time Transport Protocol (SRTP) encrypted call is made between Cisco Unified IP Phone endpoints or from a Cisco Unified IP Phone to a gateway endpoint, a lock icon is displayed on the IP phones. The lock indicates security only for the IP leg of the call. Security of the PSTN leg is not implied.

**SCCP SRST**

- Secure SCCP SRST is supported only within the scope of a single router.
- Cisco 4000 Series Integrated Services Routers support Secure SCCP SRST only on Unified SRST 12.3 and later releases. For Secure SCCP support on Unified SRST 12.3 Release:
  - Secure Cisco Jabber is not supported.
  - SRTP passthrough is not supported.
  - SDP Passthrough is not supported.
  - Video Calling is not supported.
  - Transcoding is not supported.
  - Hardware Conferencing is not supported (Only Software Conferencing is supported).
  - Secure Multicast MOH is not supported (Multicast MOH stays active, but non-secure).
  - Live MOH is not supported.
  - Secure H.323 is not supported.
  - Hot Standby Routing Protocol (HSRP) is not supported.
  - T.38 Fax Relay and Modem Relay is not supported for Unified Secure SRST.
- For call support on Voice Gateway introduced as part of Unified SRST 12.3 Release:
  - Speed Dial is not supported.
  - For a pure SCCP shared line, Hold and Remote Resume is not supported from an analog phone.
  - Full Blind Transfer mode (Configured with the CLI command `transfer-system full-blind`) is not supported.
  - Consider a call between two Analog Voice Gateways (VG A and VG B) registered on Unified Secure SRST as SCCP endpoints. If a call is already put on hold from the VG B endpoint (could be an SCCP phone too), then VG A (has to be an Analog Voice Gateway) cannot put the same call on hold (double hold). For more information, see CSCvi15203.
  - For three-way software conference related behavior and limitations, see Three-way Software Conferencing for Secure SCCP, Unified SRST Release 12.3, page 244.

**SIP SRST**

- Cisco 4000 Series Integrated Services Router supports Secure SIP SRST only on Unified SRST 12.1 and later releases.
- SRTP passthrough is not supported.
- SDP Passthrough is not supported.
- Video Calling is not supported.
- Transcoding is not supported.
- Hardware Conferencing is not supported (Only BIB Conferencing is supported).
It is mandatory to configure `security-policy secure` under `voice register global` configuration mode. Non-Secure endpoints cannot register when `security-policy secure` is configured. As such, mixed deployments of secure and non-secure endpoints is not possible.

### Information About Configuring Secure SRST

- **Benefits of Secure SRST, page 242**
- **Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router, page 242**
- **Secure SCCP SRST on Cisco 4000 Series Integrated Services Router, page 243**
- **Cisco IP Phones Clear-Text Fallback During Non-Secure SRST, page 246**
- **Signaling Security on Unified SRST - TLS, page 246**
- **Media Security on Unified SRST - SRTP, page 251**
- **Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone, page 252**
- **Secure SRST Authentication and Encryption, page 253**

### Benefits of Secure SRST

Secure Cisco Unified IP phones that are located at remote sites and that are attached to gateway routers can communicate securely with Cisco Unified Communications Manager using the WAN. But if the WAN link or Cisco Unified Communications Manager goes down, all communication through the remote phones becomes non-secure. To overcome this situation, gateway routers can now function in secure SRST mode, which activates when the WAN link or Cisco Unified Communications Manager goes down. When the WAN link or Cisco Unified Communications Manager is restored, Cisco Unified Communications Manager resumes secure call-handling capabilities.

Secure SRST provides new Cisco Unified SRST security features such as authentication, integrity, and media encryption. Authentication provides assurance to one party that another party is whom it claims to be. Integrity provides assurance that the given data has not been altered between the entities. Encryption implies confidentiality; that is, that no one can read the data except the intended recipient. These security features allow privacy for Cisco Unified SRST voice calls and protect against voice security violations and identity theft.

SRST security is achieved when:
- End devices are authenticated using certificates.
- Signaling is authenticated and encrypted using Transport Layer Security (TLS) for TCP.
- A secure media path is encrypted using Secure Real-Time Transport Protocol (SRTP).
- Certificates are generated and distributed by a CA.

### Secure SIP SRST Support on Cisco 4000 Series Integrated Services Router

For Unified SRST 12.1 and later releases, Secure SIP SRST support is introduced on the Cisco 4000 Series Integrated Services Router. As a part of the Secure SIP SRST feature on Unified SRST Release 12.1, support is provided for calls with the Transport Layer Security protocols (TLS) versions up to 1.2. Also, TLS 1.2 exclusivity is supported as part of Unified SRST Release 12.1.
The Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series is supported on the Unified Secure SIP SRST Release 12.1 configured on Cisco 4000 Series Integrated Services Routers.

For Secure SIP SRST to be supported on Cisco 4000 Series Integrated Services Routers, you need to enable the following technology package licenses on the router:

- security
- uck9

Note

For Unified SRST 12.2 and previous releases, only SIP phones are supported on the Cisco 4000 Series Integrated Services Router for Secure SIP SRST. For Unified SRST 12.3 and later releases, a mixed deployment of SIP and SCCP phones are supported on the Cisco 4000 Series Integrated Services Routers.

Secure Music On Hold for Unified Secure SRST (SIP)

From Unified SRST Release 12.1, support is introduced for Secure Music On Hold (MOH), as part of the Secure SIP SRST solution on Cisco 4000 Series Integrated Services Router. For a Secure SIP call that is put on hold, playback of Flash-based G.729 and G.711 codec format MOH files are supported. Live MOH and transcoded MOH are not supported as part of Secure MOH feature support.

Note

If the CLI command `srtpt pass-thru` is configured under the dial peer voice configuration mode, Secure MOH does not work.

Secure SCCP SRST on Cisco 4000 Series Integrated Services Router

For Unified SRST 12.3 and later releases, Secure SCCP SRST support is introduced on the Cisco 4000 Series Integrated Services Router. As a part of the Secure SCCP SRST feature on Unified SRST Release 12.3, support is provided for calls with the Transport Layer Security protocols (TLS) versions up to 1.2. Also, TLS 1.2 exclusivity is supported as part of Unified SRST Release 12.3. For more information on the TLS protocol support introduced for Secure SCCP in Unified SRST Release 12.3, see SRST Routers and the TLS Protocol, page 247.

For Secure SCCP SRST to be supported on Cisco 4000 Series Integrated Services Routers, you need to enable the following technology package licenses on the router:

- security
- uck9

The Cisco Unified IP Phone 6961 and Cisco Unified IP Phone 7962G is supported on the Unified Secure SCCP SRST Release 12.3 configured on Cisco 4000 Series Integrated Services Routers. Also, analog phones are supported for analog Voice Gateways as part of Unified Secure SCCP SRST Release 12.3. For more information on support introduced on Voice Gateways, see Secure SCCP SRST for Analog Voice Gateways, page 243.

Secure SCCP SRST for Analog Voice Gateways

For Unified SRST 12.3 and later releases on a Cisco 4000 Series Integrated Services Router, Secure SCCP support is introduced for the following Voice Gateways:

- Cisco VG202 Analog Voice Gateway
Information About Configuring Secure SRST

- Cisco VG202XM Analog Voice Gateway
- Cisco VG204 Analog Voice Gateway
- Cisco VG204XM Analog Voice Gateway
- Cisco VG224 Analog Voice Gateway
- Cisco VG300 Series Gateways (VG310, VG320, VG350)

As a part of the Secure SCCP SRST feature on Unified SRST Release 12.3, Transport Layer Security protocols (TLS) versions up to 1.2, and TLS 1.2 exclusivity is supported for Cisco VG202XM Analog Voice Gateway, Cisco VG204XM Analog Voice Gateway, Cisco VG310 Analog Voice Gateway, and Cisco VG320 Analog Voice Gateway.

For more information on configuring the Voice Gateways, see Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

Note: Cisco VG202 Analog Voice Gateway, Cisco VG204 Analog Voice Gateway, and Cisco VG224 Analog Voice Gateway only support Transport Layer Security protocols (TLS) version 1.0.

Feature Access Support for Analog Phones on Voice Gateway

For a user in basic call mode on analog phones on a voice gateway, you need to:

- Press hookflash for the first dial tone to dial an extension number to connect to a second call.
- When the second call is established, press hookflash for feature tone and #4 to transfer the call.
- When the second call is established, press hookflash for feature tone and #3 to initiate a three-way conference.
- During a three-party conference, press hookflash to drop the last conferee in Unified Communications Manager. For Unified Secure SRST, press hookflash to get feature tone and dial #2 to drop the last active party in the conference.
- When the second call is established, press hookflash for feature tone and #5 to toggle back to the previous call party.

Secure Music On Hold for Secure Unified SRST (SCCP)

From Unified SRST Release 12.3, support is introduced for Secure Music On Hold (MOH), as part of the Secure SCCP SRST functionality on Cisco 4000 Series Integrated Services Router. For a Secure SCCP call that is put on hold, playback of Flash-based G.729 and G.711 codec format MOH files are supported. Live MOH and transcoded MOH are not supported as part of Secure MOH feature support. Also, Multicast MOH is supported as non-secure on fallback from Cisco Unified Communications Manager to Unified Secure SRST.

Three-way Software Conferencing for Secure SCCP, Unified SRST Release 12.3

From Unified SRST Release 12.3, three-way software conferencing is supported for Secure SCCP endpoints on Cisco 4000 Series Integrated Services Routers. The audio codec supported as part of the three-way software conferencing for Unified SRST 12.3 Release is G.711. The support is introduced for Secure SCCP phones and Secure SCCP endpoints registered on Cisco Analog Voice Gateways.

Three-way software conferencing is supported for a pure SCCP deployment (only involving SCCP endpoints), and a mixed deployment of secure SCCP and SIP phones. The SCCP phones such as Cisco Unified IP Phone 7962, Cisco Unified IP Phone 6961, and Cisco Unified IP Phone 7975 are supported.
Information About Configuring Secure SRST

as part of this deployment. For the mixed deployment, the Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series SIP phones are supported. Three-way Software Conference is supported on TDM trunks, for SIP and SCCP endpoints on Unified Secure SRST.

You can set a limit for the maximum number of conferences that are supported. Configure the CLI command `max-conferences` under `call-manager-fallback` configuration mode to set the maximum number of conferences supported. If you do not set the maximum number of supported conferences using the command `max-conferences`, the limit is set to the default value of 8.

Router(config-cm-fallback)#max-conferences ?
<1-16> Maximum conferences to support

For a three-way software conference supported on Secure Unified SRST:

- When a secure SCCP endpoint initiates the conference or the SCCP endpoint is a conference host, the conference is created. The three-way software conference is hosted on a Unified Secure SRST router.
- When a secure SIP endpoint initiates the conference, the three-way software conference is hosted on the SIP phone.
- When the conference host puts the call on hold, the other participants in the three-way software conference will hear Music On Hold until the call is resumed by the host. Multicast MOH is played for an SCCP endpoint, whereas Unicast MOH is played for SIP endpoints.
- When the three-way software conference host is an Analog Voice Gateway endpoint, the host cannot place the conference on hold. The three-way software conference can be put on hold only by SCCP or SIP endpoints.
- When any of the conference participants (apart from the host) put the call on hold, the other participants in the three-way software conference can continue to talk.
- For a three-way software conference on Unified SRST for Secure SCCP endpoints, the conference participants can transfer the call. The conference host cannot transfer the conference call. During an alert transfer, the other two participants can continue to talk without media interruption.
- Conference Cascading is not supported for a three-way software conference on Unified Secure SRST.
- Consider a three-way software conference hosted by an Analog Voice Gateway endpoint, with SCCP A and SCCP B as the second and third conference participants, respectively. In a scenario where SCCP B places the call on hold and the conference host tries to commit the conference using hookflash (followed by FAC), the call with SCCP B is terminated and conference attempt fails.
- Consider a scenario where an Analog Phone (AP 1) registered to the Analog Voice Gateway places a call to SCCP Phone (SCCP 1) registered to Secure SCCP SRST. After placing SCCP 1 on hold, AP 1 places a call to the third participant, SCCP Phone (SCCP 2), that is registered to the same Secure SRST. Three-way Software Conferencing is established. When SCCP 2 tries to perform an alert transfer to a phone (SIP 3/ SCCP 3) and it goes unanswered, the three-way conference is lost and it becomes a one-to-one call between AP 1 and SCCP 1. Any further attempt by AP 1 to establish a three-way software conference with another phone (SCCP 4) is not supported in this scenario.

**Note**

If the failed alert transfer is by SCCP 1, then any further attempt to establish a three-way software conference with another phone will be supported.
Feature Support for Secure SRST (SCCP), Unified SRST Release 12.3

The Secure SCCP SRST on Cisco 4000 Series Integrated Services Routers and the Analog Voice Gateways introduced as part of Unified SRST Release 12.3, offers the following basic and supplementary call processing support. For a list of restrictions for Unified SRST 12.3 and later releases on Cisco Integrated Services Router Generation 2, see Restrictions for Configuring Secure SCCP SRST, page 279.

- Call Forward (Busy, No-answer, All)
- Call Hold or Resume
- Redial
- Secure MOH (Flash Based)
- Speed Dial (Only for Secure SCCP phones on Cisco 4000 Series Integrated Services Router)
- Secure Three-party Software Conference
- SIP trunks (Secure and Non-secure)
- TDM trunks
- Call Transfer (Alert, Consult, and Blind)
- Shared Line (Only for a pure SCCP-to-SCCP shared line. Mixed shared line is not supported.)
- Caller ID
- Call Waiting
- Media Inactivity

The following features are supported for Analog Voice Gateways for Fax and Modem calls on analog FXS ports:

- Fax Passthrough
- Modem Passthrough

Cisco IP Phones Clear-Text Fallback During Non-Secure SRST

- Cisco Unified SRST versions before 12.3(14)T are not capable of supporting secure connections or have security enabled. If an SRST router is not capable of SRST as a fallback mode—that is, it is not capable of completing a TLS handshake with Cisco Unified Communications Manager—its certificate is not added to the configuration file of the Cisco IP phone. The absence of a Cisco Unified SRST router certificate causes the Cisco Unified IP phone to use nonsecure (clear-text) communication when in Cisco Unified SRST fallback mode. The capability to detect and fallback in clear-text mode is built into Cisco Unified IP phone firmware. See Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways for more information on clear-text mode.

Signaling Security on Unified SRST - TLS

- SRST Routers and the TLS Protocol, page 247
- Certificates Operation on Secure SRST, page 249
- Certificates Transport from CUCM to Secure SRST, page 251
SRST Routers and the TLS Protocol

Transport Layer Security (TLS) Version 1.0 provides secure TCP channels between Cisco Unified IP phones, secure Cisco Unified SRST Routers, and Cisco Unified Communications Manager. The TLS process begins with the Cisco Unified IP Phone establishing a TLS connection when registering with Cisco Unified Communications Manager. Assuming that Cisco Unified Communications Manager is configured to fall back to Cisco Unified SRST, the TLS connection between the Cisco Unified IP Phones and the secure Cisco Unified SRST Router is also established. If the WAN link or Cisco Unified Communications Manager fails, call control reverts to the Cisco Unified SRST router.

From Unified Secure SIP SRST Release 12.1, support is introduced for SIP-to-SIP calls with Transport Layer Security up to TLS Version 1.2. For configuring TLS 1.2 exclusivity functionality, you need to configure the command `transport tcp tls v1.2` under `sip-ua` configuration mode. When you configure TLS 1.2 exclusivity on the Secure SIP SRST, any registration attempt by phones using lower versions of TLS (1.0, 1.1) are rejected.

Before Unified SRST Release 12.3, support is available only for TLS 1.0 version with Unified Secure SCCP SRST. For Unified Secure SCCP SRST Release 12.3 and later releases, support is introduced for Transport Layer Security up to TLS version 1.2. To configure a specific TLS version or TLS 1.2 exclusivity for Unified Secure SCCP SRST, you need to configure `transport-tcp-tls` under `call-manager-fallback`. When `transport-tcp-tls` is configured without specifying a version, the default behavior of the CLI command is enabled. In the default form, all the TLS versions (except TLS 1.0) are supported for this CLI command.

For Secure SIP and Secure SCCP endpoints that do not support TLS version 1.2, you need to configure TLS 1.0 for the endpoints to register to Unified Secure SRST 12.3 (Cisco IOS XE Fuji Release 16.9.1). This also means that endpoints which support 1.2 should also use the 1.0 suites.

For TLS 1.0 support on Cisco IOS XE Fuji Release 16.9.1 for SCCP endpoints, you need to specifically configure:

- `transport-tcp-tls v1.0` under `call-manager-fallback` configuration mode

For TLS 1.0 support on Cisco IOS XE Fuji Release 16.9.1 for pure SIP and mixed deployment scenarios, you need to specifically configure:

- `transport-tcp-tls v1.0` under `sip-ua` configuration mode

From Cisco IOS XE Fuji Release 16.9.1 Release, the security certificate exchange between Unified Secure SRST Release 12.3 and Unified Communications Manager does not support TLS version 1.0.

Note
Unified Communications Manager Release 11.5.1SU3 is the minimum version required to support security certificate exchange with Unified Secure SRST Release 12.3 (Cisco IOS XE Fuji Release 16.9.1).

For more information on the `transport-tcp-tls` command, see Cisco Unified SRST Command Reference (All Versions).

Note
SCCP phones and the Analog Voice Gateways VG202, VG204, and VG224 support only TLS version 1.0. For Unified Secure SRST 12.3 Release and later, TLS versions 1.1 and 1.2 are supported only for Cisco Analog Voice Gateways VG202XM, VG204XM, VG310, and VG320.

You can configure `transport-tcp-tls` under `call-manager-fallback` for Unified Secure SCCP SRST as follows:

```
Router(config-cm-fallback)#transport-tcp-tls ?
```
Information About Configuring Secure SRST

Chapter 9      Configuring Secure SRST for SCCP and SIP

v1.0  Enable TLS Version 1.0
v1.1  Enable TLS Version 1.1
v1.2  Enable TLS Version 1.2

**Note**

When you configure TLS 1.2 exclusivity on the Secure SCCP SRST, any new connection attempt by phones using lower TLS versions (1.0, 1.1) are rejected. Also, the existing TLS connections will be intact, until the connection is reset.

For Unified Secure SCCP SRST Release 12.3 and later releases, Analog Voice Gateways can register their SCCP endpoints with Transport Layer Security versions up to 1.2 (TLS 1.0, 1.1, and 1.2). For support of a specific TLS version on the analog voice gateways for Unified SRST Release 12.3 and later, you need to configure `stcapp security tls-version` under `stcapp`:

```
enable
configure terminal
stcapp security tls-version ?
exit
```

```
VG(config)#stcapp security tls-version ?
v1.0  Enable TLS Version 1.0
v1.1  Enable TLS Version 1.1
v1.2  Enable TLS Version 1.2
```

**TLS Cipher Support for Secure SRST 12.6 and Later Releases**

From Unified Secure SRST 12.6 onwards, the TLS cipher support offered on Secure SRST is modified to enhance security.

**TLS Cipher Support for SCCP/TLS (Ports 2443 and 2445)**

The following cipher suites are supported (offer and accept):
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_AES_GCM_SHA2

The following cipher suites are not supported:
- TLS_RSA_WITH_NULL_SHA

**TLS Cipher Support for SIP/TLS (Port 5061)**

The following cipher suites are supported (offer and accept):
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

The following cipher suites are not supported:
- TLS_RSA_WITH_RC4_128_MD5
TLS_DHE_RSA_WITH_AES_128_CBC_SHA1

Certificates Operation on Secure SRST

- Cisco Unified SRST Routers and PKI, page 249
- Cisco IOS Credentials Server on Secure SRST Routers, page 250
- Generating a Certificate for the Credentials Server, page 251

Cisco Unified SRST Routers and PKI

The transfer of certificates between a Cisco Unified SRST router and Cisco Unified Communications Manager is mandatory for secure SRST functionality. Public key infrastructure (PKI) commands are used to generate, import, and export the certificates for secure Cisco Unified SRST. Table 9-1 shows the secure SRST-supported Cisco Unified IP Phones and the appropriate certificate for each phone. The “Additional References” section on page 308 contains information and configurations about generating, importing, and exporting certificates that use PKI commands.

---

**Note**
Certificate text can vary depending on your configuration. You may also need CAP-RTP-00X or CAP-SJC-00X for older phones that support manufacturing installed certificate (MIC).

---

**Note**
Cisco supports Cisco IP Phones 7900 series phone memory reclamation phones that use MIC or locally significant certificate (LSC) certificates.

---

Table 9-1  **Supported Cisco Unified IP Phones and Certificates**
Chapter 9      Configuring Secure SRST for SCCP and SIP

Information About Configuring Secure SRST

Cisco IOS Credentials Server on Secure SRST Routers

Secure SRST introduces a credentials server that runs on a secure SRST router. When the client, Cisco Unified Communications Manager, requests a certificate through the TLS channel, the credentials server provides the SRST router certificate to Cisco Unified Communications Manager. Cisco Unified Communications Manager inserts the SRST router certificate in the Cisco Unified IP Phone configuration file and downloads the configuration files to the phones. The secure Cisco Unified IP Phone uses the certificate to authenticate the SRST router during fallback operations. The credentials service runs on default TCP port 2445.

Three Cisco IOS commands configure the credentials server in call-manager-fallback mode:

- credentials
- ip source-address (credentials)
- trustpoint (credentials)

Two Cisco IOS commands provide credential server debugging and verification capabilities:

- debug credentials
- show credentials
Generating a Certificate for the Credentials Server

In configuring the credentials server on the Unified Secure SRST, a certificate is required to complete the "trustpoint <trustpoint name>" configuration entry.

To generate the certificate for Credentials Server, perform the following procedures:

- Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 257
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 264
- Configuring SRST Fallback on Cisco Unified Communications Manager, page 275

Once the certificate is generated, fill in the name of the certificate (or the name of the trustpoint in IOS) in the "trustpoint" entry.

This certificate for the Credentials Server on the Secure SRST will be seamlessly exported to the Cisco Unified CM when requested in “Adding an SRST Reference to Cisco Unified Communications Manager” section on page 274.

Certificates Transport from CUCM to Secure SRST

For more information about Certificates Transport from CUCM to Secure SRST, see “Importing Phone Certificate Files in PEM Format to the Secure SRST Router” section on page 266.

Media Security on Unified SRST - SRTP

Media encryption, which uses Secure Real-Time Protocol (SRTP), ensures that only the intended recipient can interpret the media streams between supported devices. Support includes audio streams only.

If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses an RTP connection. SRTP-to-RTP fallback may occur for transfers from a secure device to a non-secure device for music-on-hold (MOH), and so on.

| Note | Secure SRST handles media encryption keys differently for different devices and protocols. All phones that are running SCCP get their media encryption keys from SRST, which secures the media encryption key downloads to phones with TLS encrypted signaling channels. Phones that are running SIP generate and store their own media encryption keys. Media encryption keys that are derived by SRST securely get sent through encrypted signaling paths to gateways over IPSec-protected links for H.323. |
| Warning | Before you configure SRTP or signaling encryption for gateways and trunks, Cisco strongly recommends that you configure IPSec because Cisco H.323 gateways, and H.323/H.245/H.225 trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Cisco Unified SRST does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed. |
Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone

Figure 9-1 shows the interworking of the credentials server on the SRST router, Cisco Unified Communications Manager, and the Cisco Unified IP Phone. Table 9-2 describes the establishment of secure SRST to the Cisco Unified IP Phone.

![Figure 9-1 Interworking of Credentials Server on SRST Router, Cisco Unified Communications Manager, and Cisco Unified IP Phone](image)

**Table 9-2 Establishing Secure SRST**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Process</th>
<th>Description or Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular Mode</td>
<td>The Cisco Unified IP Phone configures DHCP and gets the TFTP server address.</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Cisco Unified IP Phone retrieves a CTL file from the TFTP server.</td>
<td>The CTL file contains the certificates that the phone should trust.</td>
</tr>
<tr>
<td></td>
<td>The Cisco IP Phone opens a Transport Layer Security (TLS) protocol channel and registers to Cisco Unified Communications Manager.</td>
<td>Cisco Unified Communications Manager exports secure Cisco Unified SRST router information and the Cisco Unified SRST router certificate to the Cisco Unified IP phone. The phone places the certificate into its configuration. Once the phone has the Cisco Unified SRST certificate, the Cisco Unified SRST router is considered secure. See Figure 9-1.</td>
</tr>
<tr>
<td></td>
<td>If the Cisco Unified IP Phone is configured as “authenticated” or “encrypted” and Cisco Unified Communications Manager is configured in mixed mode, the phone looks for an SRST certificate in its configuration file. If it finds an SRST certificate, it opens a standby TLS connection to the default port. The default port is the Cisco Unified IP Phone TCP port plus 443; that is, port 2443 on a Cisco Unified SRST router.</td>
<td>The connection to the SRST router happens automatically, assuming there is not a secondary Cisco Unified Communications Manager and Cisco Unified SRST is configured as the backup device. See Figure 9-1. Cisco Unified Communications Manager should be configured in mixed mode, which is its secure mode.</td>
</tr>
</tbody>
</table>
In case of WAN failure, the Cisco Unified IP Phone starts Cisco Unified SRST registration.

<table>
<thead>
<tr>
<th>SRST Mode</th>
<th>The Cisco Unified IP Phone registers with the SRST router at the default port for secure communications.</th>
</tr>
</thead>
</table>

### Secure SRST Authentication and Encryption

Figure 9-2 illustrates the process of secure SRST authentication and encryption, and Table 9-3 describes the process.

#### Figure 9-2 Secure Cisco Unified SRST Authentication and Encryption

![Diagram of Secure Cisco Unified SRST Authentication and Encryption](image)

#### Table 9-3 Overview of the Process of Secure SRST Authentication and Encryption

<table>
<thead>
<tr>
<th>Process Steps</th>
<th>Description or Detail</th>
</tr>
</thead>
</table>
| 1.            | The CA server, whether it is a Cisco IOS router CA or a third-party CA, issues a device certificate to the SRST gateway, enabling credentials service. Optionally, the certificate can be self-generated by the SRST router using a Cisco IOS CA server.  
               | The CA router is the ultimate trustpoint for the Certificate Authority Proxy Function (CAPF). For more information on CAPF, see Cisco Communications Manager Security Guide.                                             |
| 2.            | The CAPF is a process where supported devices can request a locally significant certificate (LSC). The CAPF utility generates a key pair and certificate that is specific for CAPF, copies this certificate to all Cisco Unified Communications Manager servers in the cluster, and provides the LSC to the Cisco Unified IP Phone.  
               | An LSC is required for Cisco Unified IP Phones that do not have a manufacturing installed certificate (MIC). The Cisco 7970 is equipped with a MIC and therefore does not need to go through the CAPF process.                       |
| 3.            | Cisco Unified Communications Manager requests the SRST certificate from credentials server, and the credentials server responds with the certificate.                                                                                           |
How to Configure Secure Unified SRST

The following configuration sections ensure that the secure Cisco Unified SRST Router and the Cisco Unified IP Phones can request mutual authentication during the TLS handshake. The TLS handshake occurs when the phone registers with the Cisco Unified SRST Router, either before or after the WAN link fails.

This section contains the following procedures:

- Preparing the Cisco Unified SRST Router for Secure Communication, page 255
- Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router, page 274
- Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 277
- Configuring Secure SCCP SRST, page 279
- Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293

### Table 9-3 Overview of the Process of Secure SRST Authentication and Encryption (continued)

<table>
<thead>
<tr>
<th>Process Steps</th>
<th>Description or Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>For each device, Cisco Unified CM uses the TFTP process and inserts the certificate into the SEPMACxxxx.cnf.xml configuration file of the Cisco Unified IP Phone.</td>
</tr>
<tr>
<td>5.</td>
<td>Cisco Unified CM provides the PEM format files that contain phone certificate information to the Cisco Unified SRST router. Providing the PEM files to the Cisco Unified SRST router is done manually. See “Cisco IOS Credentials Server on Secure SRST Routers” section on page 250 for more information. When the Cisco Unified SRST router has the PEM files, the Cisco Unified SRST Router can authenticate the IP phone and validate the issuer of the IP phones certificate during the TLS handshake.</td>
</tr>
<tr>
<td>6.</td>
<td>The TLS handshake occurs, certificates are exchanged, and mutual authentication and registration occurs between the Cisco Unified IP Phone and the Cisco Unified SRST Router.</td>
</tr>
<tr>
<td>a.</td>
<td>The Cisco Unified SRST Router sends its certificate, and the phone validates the certificate to the certificate that it received from Cisco Unified CM in Step 4.</td>
</tr>
<tr>
<td>b.</td>
<td>The Cisco Unified IP Phone provides the Cisco Unified SRST Router the LSC or MIC, and the router validates the LSC or MIC using the PEM format files that it was provided in Step 5.</td>
</tr>
</tbody>
</table>

Note

The media is encrypted automatically after the phone and router certificates are exchanged and the TLS connection is established with the SRST router.
Preparing the Cisco Unified SRST Router for Secure Communication

The following tasks prepare the Cisco Unified SRST Router to process secure communications.

- Configuring a Certificate Authority Server on a Cisco IOS Certificate Server, page 255 (optional)
- Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 257 (required)
- Disabling Automatic Certificate Enrollment, page 261 (required)
- Verifying Certificate Enrollment, page 262 (optional)
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 264 (required)
- Troubleshooting Credential Settings, page 266
- Importing Phone Certificate Files in PEM Format to the Secure SRST Router, page 266

Configuring a Certificate Authority Server on a Cisco IOS Certificate Server

For Cisco Unified SRST Routers to provide secure communications, there must be a CA server that issues the device certificate in the network. The CA server can be a third-party CA or one generated from a Cisco IOS certificate server.

The Cisco IOS certificate server provides a certificate generation option to users who do not have a third-party CA in their network. The Cisco IOS certificate server can run on the SRST router or on a different Cisco IOS router.

If you do not have a third-party CA, full instructions on enabling and configuring a CA server can be found in the Cisco IOS Certificate Server documentation. A sample configuration is provided below.

**SUMMARY STEPS**

1. `crypto pki server cs-label`
2. `database level {minimal | names | complete}
3. `database url root-url`
4. `issuer-name DN-string`
5. `grant auto`
6. `no shutdown`
### 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>crypto pki server cs-label</code></td>
<td>Enables the certificate server and enters certificate server configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router (config)# crypto pki server srstcaserver</code></td>
<td>If you manually generated an RSA key pair, the <code>cs-label</code> argument must match the name of the key pair.</td>
</tr>
</tbody>
</table>

| **Note** | For more information on the certificate server, see the *Cisco IOS Certificate Server* documentation. |

| **Step 2**         |         |
| `database level [minimal | names | complete]` | Controls what type of data is stored in the certificate enrollment database. |
| **Example:**       |         |
| `Router (cs-server)# database level complete` | - **minimal**: Enough information is stored only to continue issuing new certificates without conflict; this is the default. |
|                     | - **names**: In addition to the information given in the minimal level, the serial number and subject name of each certificate are stored. |
|                     | - **complete**: In addition to the information given in the minimal and names levels, each issued certificate is written to the database. |

| **Note** | The `complete` keyword produces a large amount of information; if it is issued, you should also specify an external TFTP server on which to store the data using the `database url` command. |

| **Step 3**         |         |
| `database url root-url` | Specifies the location where all database entries for the certificate server will be written. After you create a certificate server using the `crypto pki server` command, use this command to specify a combined list of all the certificates that have been issued. The `root-url` argument specifies the location where database entries are written. |
| **Example:**       |         |
| `Router (cs-server)# database url nvram` | - The default location for the database entries to be written is flash; however, NVRAM is recommended for this task. |

| **Step 4**         |         |
| `issuer-name DN-string` | Sets the CA issuer name to the specified distinguished name (DN-string). The default value is as follows: |
| **Example:**       |         |
| `Router (cs-server)# issuer-name CN=srstcaserver` | `issuer-name CN=cs-label`. |
How to Configure Secure Unified SRST

Examples

The following example reflects one way of generating a CA:

```
Router(config)# crypto pki server srstcaserver
Router(cs-server)# database level complete
Router(cs-server)# database url nvram
Router(cs-server)# issuer-name CN=srstcaserver
Router(cs-server)# grant auto

% This will cause all certificate requests to be automatically granted.
Are you sure you want to do this? [yes/no]: y
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: y
% Generating 1024 bit RSA keys ...[OK]
% Certificate Server enabled.
```

Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server

The secure Cisco Unified SRST Router needs to define a trustpoint; that is, it must obtain a device certificate from the CA server. The procedure is called certificate enrollment. Once enrolled, the secure Cisco Unified SRST Router can be recognized by Cisco Unified Communications Manager as a secure SRST router.

There are three options to enroll the secure Cisco Unified SRST Router to a CA server: autoenrollment, cut and paste, and TFTP. When the CA server is a Cisco IOS certificate server, autoenrollment can be used. Otherwise, manual enrollment is required. Manual enrollment refers to cut and paste or TFTP.

Use the enrollment url command for autoenrollment and the crypto pki authenticate command to authenticate the SRST router. Full instructions for the commands can be found in the Certification Authority Interoperability Commands documentation. An example of autoenrollment is available in the Certificate Enrollment Enhancements feature. A sample configuration is provided in the “Examples” section on page 260.

SUMMARY STEPS

1. crypto pki trustpoint name
2. rsakeypair keypair-label
3. enrollment url url
4. revocation-check method
5. exit
6. crypto pki authenticate name
7. crypto pki enroll name
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> crypto pki trustpoint name</td>
<td>Declares the CA that your router should use and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# crypto pki trustpoint srstca</td>
<td>- The name provided will be the same as the trustpoint name that will be declared in the “Enabling Credentials Service on the Secure Cisco Unified SRST Router” section on page 264.</td>
</tr>
<tr>
<td><strong>Step 2</strong> rsakeypair keypair-label</td>
<td>To specify a named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint, use the rsakeypair command in trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-trustp)# rsakeypair srstkey 2048</td>
<td>- For TLS 1.2 version, the RSA key length is set to 2048 bits.</td>
</tr>
<tr>
<td><strong>Step 3</strong> enrollment url url</td>
<td>Specifies the enrollment parameters of your CA.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(ca-trustpoint)# enrollment url <a href="http://10.1.1.22">http://10.1.1.22</a></td>
<td>- <strong>url url</strong>: Specifies the URL of the CA to which your router should send certificate requests.</td>
</tr>
<tr>
<td></td>
<td>- If you are using Cisco proprietary SCEP for enrollment, <strong>url</strong> must be in the form file://CA_name, where <strong>CA_name</strong> is the host Domain Name System (DNS) name or IP address of the Cisco IOS CA.</td>
</tr>
<tr>
<td></td>
<td>- If you used the procedure documented in the “Configuring a Certificate Authority Server on a Cisco IOS Certificate Server” section on page 255, the URL is the IP address of the certificate server router configured in Step 1. If a third-party CA was used, the IP address is to an external CA.</td>
</tr>
<tr>
<td><strong>Step 4</strong> revocation-check method1</td>
<td>Checks the revocation status of a certificate. The argument <strong>method1</strong> is the method used by the router to check the revocation status of the certificate. For this task, the only available method is <strong>none</strong>. The keyword <strong>none</strong> means that a revocation check will not be performed and the certificate will always be accepted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(ca-trustpoint)# revocation-check none</td>
<td>- Using the <strong>none</strong> keyword is mandatory for this task.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits ca-trustpoint configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action | Purpose
--- | ---
**Step 6** | crypto pki authenticate name
**Example:**
Router(config)# crypto pki authenticate srstca
| Authenticates the CA (by getting the certificate from the CA).
* Takes the name of the CA as the argument.

**Step 7** | crypto pki enroll name
**Example:**
Router(config)# crypto pki enroll srstca
| Obtains the SRST router certificate from the CA.
* Takes the name of the CA as the argument.

### Examples

The following example autoenrolls and authenticates the Cisco Unified SRST router:

```bash
Router(config)# crypto pki trustpoint srstca
Router(ca-trustpoint)# enrollment url http://10.1.1.22
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate srstca
Certificate has the following attributes:
Fingerprint MD5: 4C894B7D 71DBA53F 50C65FD7 75DDBFCA
Fingerprint SHA1: 5C3B6B9E EFA40927 9DF6A826 5BDA618A BF39F291
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
Router(config)# crypto pki enroll srstca
% 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 fully-qualified domain name in the certificate will be: router.cisco.com
% The subject name in the certificate will be: router.cisco.com
% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: D0B9E79C
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 0573FB2 98CD1AD0 F37D591A C595252D A17523C1
Sep 29 00:41:57.339: %PKI-6-CERTRET: Certificate received from Certificate Authority
```
Disabling Automatic Certificate Enrollment

The command `grant auto` allows certificates to be issued and was activated in the optional task documented in the “Configuring a Certificate Authority Server on a Cisco IOS Certificate Server” section on page 255.

Note

You should disable the `grant auto` command so that certificates cannot be continually granted.

SUMMARY STEPS

1. `crypto pki server cs-label`
2. `shutdown`
3. `no grant auto`
4. `no shutdown`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> crypto pki server <em>cs-label</em></td>
<td>Enables the certificate server and enters certificate server configuration mode. Note If you manually generated an RSA key pair, the <em>cs-label</em> argument must match the name of the key pair.</td>
</tr>
</tbody>
</table>

Example:

Router (config)# crypto pki server srstcaserver

**Step 2** shutdown | Disables the Cisco IOS certificate server. |

Example:

Router (cs-server)# shutdown

**Step 3** no grant auto | Disables automatic certificates to be issued to any requestor. |

Example:

Router (cs-server)# no grant auto

- This command was for use during enrollment only and thus needs to be removed in this task.

**Step 4** no shutdown | Enables the Cisco IOS certificate server. |

Example:

Router (cs-server)# no shutdown

- You should issue this command only after you have completely configured your certificate server.

What to Do Next

For manual enrollment instructions, see the *Manual Certificate Enrollment (TFTP and Cut-and-Paste)* feature.
Verifying Certificate Enrollment

If you used the Cisco IOS certificate server as your CA, use the `show running-config` command to verify certificate enrollment or the `show crypto pki server` command to verify the status of the CA server.

SUMMARY STEPS

1. `show running-config`
2. `show crypto pki server`
# Chapter 9 Configuring Secure SRST for SCCP and SIP

## How to Configure Secure Unified SRST

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show running-config</td>
<td>Use the <code>show running-config</code> command to verify the creation of the CA server (01) and device (02) certificates. This example shows the enrolled certificates.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router# show running-config
.
.
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
308201AD 30820116 A0030201 02020102 300D0609
2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365
72766572 301E170D 30343034
31323139 35323233 5A170D30 35303431 32313935
3232335A 30343132 300F0603
55040513 08433042 39453739 43301F06 092A8648
86F70D01 09021612 6A17136F
32363931 2E636973 636F2E63 6F6D303C 300D0609
2A864886 F70D0101 01050030
4B003048 024100D7 0CC354FB 5F7131E7 7A253C3F2
056E0485 22896D36 6CA70C19
C98F9B9F AE9D1F9B D4BB7A67 F3251174 193B81A3
12946123 E51CCD7 A23B5155
F32ED743 3FBB8902 03010001 A330302E 300B0603
551D0F04 04030205 A031F06
01551D23 04183016 62144829 CB97AD60 180D5467
FC293963 C2470691 F9BD300D
6092A86 4886F70D 01010405 0038181 07EB48E
CAE9E1B3 D1E7A185 D7F0D565
CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D
99C9BD27 8657C88B 62DBDE8E
FB2B18A0 34AF6564 1239473 41478AFC A865E6D1
AC51B2DE 8657C88B 62DBDE8E
B586FEB7 00C358D4 EFDD8D43 3F423141 C2D331D3
C849A6F 600734D8 0D30300A EA3C206D CF |
```

Use the `show running-config` command to verify the creation of the CA server (01) and device (02) certificates. This example shows the enrolled certificates.
How to Configure Secure Unified SRST

Enabling Credentials Service on the Secure Cisco Unified SRST Router

Once the Cisco Unified SRST Router has its own certificate, you need to provide Cisco Unified Communications Manager the certificate. Enabling credentials service allows Cisco Unified Communications Manager to retrieve the secure SRST device certificate and place it in the configuration file of the Cisco Unified IP Phone.

Activate credentials service on all Cisco Unified SRST Routers.

A security best practice is to protect the credentials service port using Control Plane Policing. Control Plane Policing protects the gateway and maintains packet forwarding and protocol states despite a heavy traffic load. For more information on control planes, see the Control Plane Policing documentation. In addition, a sample configuration is given in the “Control Plane Policing: Example” section on page 292.

Command or Action | Purpose
--- | ---
show crypto pki server | Use the show crypto pki server command to verify the status of the CA server after a boot procedure.

Example:
Router# show crypto pki server
Certificate Server srstcaserver:
Status: enabled
Server’s configuration is locked (enter “shut” to unlock it)
Issuer name: CN=srstcaserver
CA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00
Granting mode is: auto
Last certificate issued serial number: 0x2
CRL NextUpdate timer: 14:54:57 PST Jan 19 2005
Current storage dir: nvram
Database Level: Complete - all issued certs written as <serialnum>.cer
# How to Configure Secure Unified SRST

## SUMMARY STEPS

1. credentials
2. ip source-address ip-address [port port]
3. trustpoint trustpoint-name
4. exit

## 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>credentials</td>
<td>Provides the Cisco Unified SRST Router certificate to Cisco Unified Communications Manager and enters credentials configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# credentials</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>ip source-address ip-address [port port]</td>
<td>Enables the Cisco Unified SRST Router to receive messages from Cisco Unified Communications Manager through the specified IP address and port.</td>
</tr>
</tbody>
</table>
| Example: | Router(config-credentials)# ip source-address 10.1.1.22 port 2445 | - ip-address: The IP address is the pre-existing router IP address, typically one of the addresses of the Ethernet port of the router.  
- port port: (Optional) The port to which the gateway router connects to receive messages from Cisco Unified Communications Manager. The port number is from 2000 to 9999. The default port number is 2445. |
| Step 3 | trustpoint trustpoint-name | Specifies the name of the trustpoint that is to be associated with the Cisco Unified SRST Router certificate. The trustpoint-name argument is the name of the trustpoint and corresponds to the SRST device certificate. |
| Example: | Router(config-credentials)# trustpoint srstca | - The trustpoint name should be the same as the one declared in the “Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server” section on page 257. |
| Step 4 | exit | Exits credentials configuration mode. |
| Example: | Router(config-credentials)# exit | |

### Examples

- Router(config)# credentials
- Router(config-credentials)# ip source-address 10.1.1.22 port 2445
- Router(config-credentials)# trustpoint srstca
- Router(config-credentials)# exit
Troubleshooting Credential Settings

The following steps display credential settings or set debugging on the credential settings of the Cisco Unified SRST Router.

**SUMMARY STEPS**

1. show credentials
2. debug credentials

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show credentials</td>
<td>Use the show credentials command to display the credential settings on the Cisco Unified SRST Router that are supplied to Cisco Unified Communications Manager for use during secure Cisco Unified SRST fallback.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show credentials</td>
<td></td>
</tr>
<tr>
<td>Credentials IP: 10.1.1.22</td>
<td></td>
</tr>
<tr>
<td>Credentials PORT: 2445</td>
<td></td>
</tr>
<tr>
<td>Trustpoint: srstca</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> debug credentials</td>
<td>Use the debug credentials command to set debugging on the credential settings of the Cisco Unified SRST Router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# debug credentials</td>
<td></td>
</tr>
<tr>
<td>Credentials server debugging is enabled</td>
<td></td>
</tr>
<tr>
<td>Router#</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:50.903: Credentials service: Start TLS Handshake 1 10.1.1.13 2187</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:50.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:51.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr</td>
<td></td>
</tr>
<tr>
<td>Sep 29 01:01:52.907: Credentials service: TLS Handshake completes.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

Use the following commands to show if a certificate cannot be found (you are missing a certificate that you are trying to authenticate) or to show that a particular certificate has matched (so you know what certificate the router used to authenticate a phone):

- debug crypto pki messages
- debug crypto pki transactions

**Importing Phone Certificate Files in PEM Format to the Secure SRST Router**

This task completes the tasks required for Cisco IP Unified Phones to authenticate secure SRST.
Cisco Unified Communications Manager 4.X.X and Earlier Versions

For systems running Cisco Unified Communications Manager 4.X.X and earlier versions, the secure Cisco Unified SRST Router must retrieve phone certificates so that it can authenticate Cisco Unified IP phones during the TLS handshake. Different certificates are used for different Cisco Unified IP Phones. Table 9-1 lists the certificates needed for each type of phone.

Certificates must be imported manually from Cisco Unified Communications Manager to the Cisco Unified SRST Router. The number of certificates depends on the Cisco Unified Communications Manager configuration. Manual enrollment refers to cut and paste or TFTP. For manual enrollment instructions, see the Manual Certificate Enrollment (TFTP and Cut-and-Paste) feature. Repeat the enrollment procedure for each phone or PEM file.

For Cisco Unified Communications Manager 4.X.X and earlier versions, certificates are found by going to the menu bar in Cisco Unified Communications Manager, choose Program Files > Cisco > Certificates.

Open the .0 files with Windows WordPad or Notepad, and copy and paste the contents to the SRST router console. Then, repeat the procedure with the .pem file. Copy all the contents that appear between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".


Cisco Unified Communications Manager 5.0 and Later Versions

Systems running Cisco Unified CM 5.0 and later versions require four certificates (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) in addition to the requirements listed in Table 9-1, which must be copied and pasted to Cisco Unified SRST Routers.

Note CiscoRootCA is also called CiscoRoot2048CA.

Prerequisites

You must have certificates available when the last configuration command (crypto pki authenticate) issues the following prompt:

Enter the base 64 encoded CA certificate.
End with a blank line or the word 'quit' on a line by itself

For Cisco Unified CM 5.0 and later versions, perform the following steps:

---

**Step 1** Login to Cisco Unified Communications Manager.

**Step 2** Go to Security > Certificate Management > Download Certificate/CTL.

**Step 3** Select Download Trust Cert and click Next.

**Step 4** Select CAPF-trust and click Next.

**Step 5** Select CiscoCA and click Next.

**Step 6** Click Continue.

**Step 7** Click the file name.
How to Configure Secure Unified SRST

Step 8 Copy all the contents that appear between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” to a location where you can retrieve it later.

Step 9 Repeat Steps 5 to 8 for CiscoManufactureCA, CiscoRootCA2048, and CAPF.

Cisco Unified Communications Manager 6.0 and Later Versions

From Cisco Unified Communications Operating System Administration, download all certificates listed under CAPF-trust, including Cisco_Manufacturing_CA, Cisco_Root_CA_2048, CAP-RTP-001, CAP-RTP-002, CAPF, and CAPF-xxx. Also download any CAPF-xxx certificates that are listed under CallManager-trust and not under CAPF-trust.

For instructions on downloading certificates, see the “Security” chapter in the appropriate version of Cisco Unified Communications Operating System Administration Guide.

Authenticating the Imported Certificates on the Cisco Unified SRST Router

To authenticate certificates on the Cisco Unified SRST router, perform these steps.

Restrictions

HTTP automatic enrollment from Cisco Unified Communications Manager through a virtual web server is not supported.

SUMMARY STEPS

1. crypto pki trustpoint name
2. revocation-check none
3. enrollment terminal
4. exit
5. crypto pki authenticate name
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> crypto pki trustpoint name</td>
<td>Declares the CA that your router should use and enters</td>
</tr>
<tr>
<td></td>
<td>ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• name: Enter the name of each certificate individually</td>
</tr>
<tr>
<td></td>
<td>(for example, CAPF, CiscoCA, CiscoManufactureCA, and</td>
</tr>
<tr>
<td></td>
<td>CiscoRootCA2048).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router (config)# crypto pki trustpoint CAPF</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> revocation-check none</td>
<td>Checks the revocation status of a certificate using the</td>
</tr>
<tr>
<td></td>
<td>selected method.</td>
</tr>
<tr>
<td></td>
<td>• Using the <strong>none</strong> keyword is mandatory for this task. The</td>
</tr>
<tr>
<td></td>
<td>keyword <strong>none</strong> means that a revocation check is not performed and</td>
</tr>
<tr>
<td></td>
<td>the certificate is always accepted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# revocation-check none</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> enrollment terminal</td>
<td>Specifies manual cut-and-paste certificate enrollment.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits ca-trustpoint configuration mode and returns to</td>
</tr>
<tr>
<td></td>
<td>global configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> crypto pki authenticate name</td>
<td>Authenticates the CA (by getting the certificate from the</td>
</tr>
<tr>
<td></td>
<td>CA).</td>
</tr>
<tr>
<td></td>
<td>• Enter the same <strong>name</strong> argument used in the crypto pki</td>
</tr>
<tr>
<td></td>
<td>trustpoint command in <strong>Step 1</strong>.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki authenticate CAPF</td>
<td></td>
</tr>
</tbody>
</table>

What to Do Next

Update the certificates in Cisco Unified CM. See the “Configuring a Secure Survivable Remote Site Telephony (SRST) Reference” chapter in the appropriate version of *Cisco Unified Communications Manager Security Guide*.

Examples

This section provides the following:

- Cisco Unified Communications Manager 4.X.X and Earlier Versions: Example, page 270
- Cisco Unified Communications Manager 5.0 and Later Versions Example, page 272
Cisco Unified Communications Manager 4.X and Earlier Versions: Example

The following example shows three certificates (Cisco 7970, 7960, PEM) imported to the Cisco Unified SRST Router:

```plaintext
Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(config)# exit
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself.

```
MIIDqDCCApCgAwIBAgIQNT+yS9cPFKNGwfoPzrHLWdTFANBqkqZkI9gW0BAQUDAn
MRWwFAYUQQQEQW1daXNjbyBTexZNQz1mMRwB9yDQGDBwttDQVATULRQ7FmApfWf
wQw0zrGWMTayMD4aND1aFw0y1XeMbMTayMD1iMzaMC4xPjAIiBGiQvbAotDUnpc2N
IFN5c3r1bxMNFDAS8QNBVMBTCONBUC1VSFA1MDAYMIIIBPDBgkqkI9gW0BAGEP
AAACQA0QAMBIKCAQACXARC21B1K19/w/2NZVvpgcPrpWlc7CCy7q1h9i81S5ZzdNgQ
2M4Cufg0sNz0yXGQ1iAYefCR3ECMB3f5A+x7nX1EuB87U66V/K+7S80wUCW0Uht1
AVrFv5NQ23YDN0NQ5M0n0BIn18T8F55E5E2yVac0XGne777S1b1dejTvTQYP2GPNX
Qygh+ZQ1GFD9ZRhMi8F8Duv2M2e+1+Sgmg0Q9cIk6gkq9H93/XCS1JhuZNNv8Gd+mv
Hth2P6K2zqKXAAStQRLSZX3jN8b8tve3J3g1+Sj+9+F6KKK2P0D1.wHcrkckcUH8b7g
1+u/0+1sw0jUDzpp725s22rnehkmH1GlGFk8fkgCUvbA6OBwzCBwDLB6yH9Q8E
BANCAYyYyqWYDvRTOAQ/A1BA8wzB/zaB8y/9jVQ48IFU9UsrcI40uJlDgmK65LWa5Lal
Mr7m5ywbYVDR0fBqgwlzJ8k0Ok1IQYtahhCovLV2hNucClyHAtMDAYMII1ncRw
b0VvbVwqVQFLOUUUCWMDJ5J3shi9maWwciO1v8VFJXJYAcnRwLTAM1iDZXJO
RW5by2uxIEXNCUICIFvMTAYMDAyM0ByDQgkgk8rBGEA8Y13FFEQEAvIABNABDQgkkhk1G
9G8wBAQPAAAOAQgBqBtMoN87Ta0Mhj7sVL/5u5VChlyyvU6f6fqiJLWNj12p2ViIhm
E+DlXwM5S5JaqtuaSd/m/xz0pCkJM4ZWbW6VqeiqGj/kJUZeB5JS13KAE7heg
tup4HP/2f8wkPAD40DalG582DNNm0mVOoCQUMH2UKPKseEQ9sw6G7s7uhMN4y4C
PNmRQ8PPk/L69hStScZHTgEPxEG8Y112qCy3h/ERwbmp0OHz+dx20PuJ816G1I+L39l
aRejeD708f2yZ9wemw9Ew2htn2KzseIni1Yqq1Dlx9yuP838c18KHwcmj4DVTXux
V6Y47H1yv/GJCM8PvdgyE1kEXBGTFIN1HpPiaG9tq==
```

Certificate has the following attributes:

```
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(config)# exit

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself.

```
MIICKDCCAzGwAIgBq1C8WEwDQYJKoZIhvcNAQEFBQAwQDELMAkGA1UEBhMCVVMx
GjAYbGnvRBoeEUUnPC2Nv1F5NC31lhM6mg95jLRwUDvQDYDBwQxQVBLdEDN0Qw
QzAwhCnMDQwN2EIlmJ20DMFyWncNMKw4WkyMj1z0DMFyWjBAMQswCQYDVQQGEwJV
UzEA6hBGA1UECHMRq21yZ2Bq123ZgVtCvBjEmXKFTATBcNvBTMDenB2UyNQ3
RRDDMCBn2ANBskj19gW0BAQEAFAOIBjAQgYkCgYEo0hMV029ENMe11YGY1
i2TwW31ENk/eh2hV69p9eqBlqT/fP9eA0GW0Z5b05PetdU+BcmPnndeoAeSpf3Z+x
+z5hLEIRHRQmD2ynamoY9uwuxwC8NgWq1w147YHj17t5/5C/0B76daxC4B5NBo6
k0dq6qQnr0131p59kaC8hL/KcAWEAAaAmdC8wDy7DVQPA9J/BAQDQgKREM300A1td
slQjW6MBBCaQAQGAFw8EMBwwBmGbrgBqEFQcDBTHABqkqkI9gW0BAQUDAn
Ql5M5N6iZepSB09Qm9YvFMRV2YrsrSwxZHu0g9JQ3MS8T8t1w9NqVa47hS31F5a8
vYU101dIdf0r4o+/E07kkmmFEBMTA5r85M7Uwjb8A8g24qA3Rq2aDwudGJ9W7FH
GgfU lav9AIkxwsxV1vMsLD2yC0Qw3JQ7B2q=
```

Certificate has the following attributes:

Fingerprint MD5: 4B9636DF 0F3BA687 5F54BE72 24762DBC
Chapter 9      Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

Fingerprint SHA1: A9917775 F86B2B8A 3E52BBB8 28E8E2CD
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint PEM
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate PEM

Enter the base 64 encoded CA certificate.
End with a blank line or the word 'quit' on a line by itself

Certificate has the following attributes:
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Use the show crypto pki trustpoint status command to show that enrollment has succeeded
and that five CA certificates were granted. The five certificates include the three
certificates just entered and the CA server certificate and the SRST router certificate.

Router# show crypto pki trustpoint status
Keys generated .............. Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None

Trustpoint PEM:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-001,o=Cisco Systems
Fingerprint MD5: 233C8E83 8632EA4E 76D79FE8 FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8B2 25990732 227631BE
State:
Keys generated .............. Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None

Trustpoint srtscaserver:
Issuing CA certificate configured:
Subject Name:
cn=srtscaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
State:
Keys generated .............. Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srtscaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
Router General Purpose certificate configured:
Subject Name:
serialNumber=F3246544+hostname=c2611XM-sSRST.cisco.com
Fingerprint: 35471295 1C907EC1 45B347BC 7A9C4B86
State:
Keys generated .............. Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... Yes

Cisco Unified Communications Manager 5.0 and Later Versions Example

The following example shows the configuration for the four certificates (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) that are required for systems running Cisco Unified Communications Manager 5.0:

Router(config)# crypto pki trustpoint CAPF
Router(config-ca-trustpoint)# revocation-check none
Router(config-ca-trustpoint)# enrollment terminal
Router(config-ca-trustpoint)# exit
Router(config)# crypto pki authenticate CAPF

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKjCCAZOgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQTELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4RUFEM
MARYwFAYDVQQDEw1DQVBGLTU4RUFEMkY4MDAwMDExMTIzMTMwLjEwLjAuMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC99KgZT94qhoz4bOB
Chapter 9  Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

f8Z0tYwT2L4L++mC64O3s3AshDi8xe8Y8sN/f/ZKRRhNIXbLk4SwAfXnxHkJBgKZnWtSkqrj/3JDhOXtqowYT8VS2sC69g8aX091skKl3+Tpwzr2T/mDXV6CeoAKN+mcchgcrmN08kamOOIG80sQc4L6XzQIDAQABozEwLzA0BgnNVHQ8BAf8EBAMCAoQwHqYD quit
Certificate has the following attributes:
Fingerprint MD5: 1951DJ4E 76D79FEB FFB061C6 233C8E33
Fingerprint SHA1: 222891BE 47AB8F82 581D2AB 25990732
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoCA
Router(ca-trustpoint)# revocation-check none
Router(config)# exit
Router(config)# crypto pki authenticate CiscoCA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCCApCgAwIBAgIQAhL5YBU9b59QOFAgMrcjVjYANBgqhkkiG9wBAQUFAFAU
MRywFAYDVQQKEw1DaXNjbyBTeXN0ZW1lMRQwBggYDVQQDEwJQVAtUlRQLTAwMTAe
Vd54qIpc/hQdJ5bWbrIFkCvyhIsw7vwnPsLu1jKw21r2cP0UXXyGhhSeX8H4vQgpDPQ
NnYy7aJkK435DF4t2n37n8/7v1rU0x3mdbcBEdBAb825Yo1a8sk12shN7/Ydmt
Vnyp0mdNZNxmeHjIGqV0U3U6GvC0+Kly1dUu1ogYJNPyLkqx7wgcCgsjHdHr3
A+uw1lu1gsGqSnMweAow8+6hvMw1APeufgZ2yiewIAE60wczBwDLDAGbNVHQ8E
c6As/7f5mQKlCmBrTrystMUb9FvDNbnEbj3jitaIC5fg8/S9RS6C1Qy7ZPhn5tUjY
WXzeYSXPrxcb0U7tt7tQJ1JqgDONAUKLoZaU7t7VDSH3hD4+VJjmLyysaLUNksGFRR
phzZrsVUI1k7gdQCP1kLKAS4f5bkrq3r/65/SpX6/gAo1jBKlxP72WXpCUG
laU9cURLP95NDOFJN1/848s3ps7cVidcogowoP==
Certificate has the following attributes:
Fingerprint MD5: 21956CBR 4B9706DF 0F3BA6B7 7P54A272
Fingerprint SHA1: A9917775 F86BB37A 7H130ED2 3E528BB8 2868EC2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoManufactureCA
Router(config)# crypto pki authenticate CiscoManufactureCA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIE2TCCA8GAgwIBAgIKAmKlnswAAAAAASBNBkgkhiG9w0BAQUFADA1MRYwPAYD
D/g2q5k5k6NhYN0MDR9exIXBSZ5c2/G7FNCXtc6jUAAQIBA6GC
AecwgPhq/aJ1lAGUdweBE/wqM1MYBAf8CQAAwHQYDVR0 DB6Q8OEBYFNDF1iarT02Z7KG4
kcffVctcWx/daMAsaG1U5w4EaWaIbH/gAQBgkr8gEEAY13FQERAwVIBADA2Ebgk8gEE
AY13FJ1EB4KAFMAdqBiAEMQTaFbqVHSMEDGADwBqN88ygh/aQKBgq7Sjug1VbF
2nsvqjBDBgNVHR88EPDAA6MD1gNgA0hJnoHrO1B8vd3d3LmNpc2NvLmNvbiZ9ZmN
m2xZz9NN1cm0less9w2akV3Jz6L2Ny2EyEQ4LmYqDBgBgq2BEBqRCdARQFMDITwQAIKkY
BQHUMARKGKn6ohJiAAlly93d3cyuV2yZ8yu29tL3V1YVyxXR553B8s9JzX0czy9j
cmN0MhrJ1dC052JIXvXAYDYR0gBFUWdZfBBgorBggEAAQkVQAMewQQYKwYBBQHU
I+il66tvaNS6g04cT3nPpB+rNhC586WV02jG9PML9d7QWbch2RvhFDONOEDyepe3
0OfTc79F0o4ipUs4eakqjJN90n6jVnWxxmEPxnc5JlunGdG7jaubBEEDpH6GC/f08
How to Configure Secure Unified SRST

Chapter 9 Configuring Secure SRST for SCCP and SIP

### How to Configure Secure Unified SRST

Certificate has the following attributes:
- Fingerprint MD5: 0F3BA6B7 4B9636DF 5F54BE72 24762SBR
- Fingerprint SHA1: L92BB37A S9919925 5C130ED2 3E528UF8 286E8C2D

To accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
Certificate successfully imported.

```
Router(config)# crypto pki trustpoint CiscoRootCA2048
Router(config-trustpoint)# revocation-check none
Router(config-trustpoint)# enrollment terminal
Router(config-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoRootCA2048
```

Certificate has the following attributes:
- Fingerprint MD5: 2G3LZ6B7 2R1995ER 6KE4782 3E528SBR
- Fingerprint SHA1: M9912245 5C130ED2 3E528UF8 956E85H

To accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
Certificate successfully imported.

### Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router

The following tasks are performed in Cisco Unified Communications Manager:
- **Adding an SRST Reference to Cisco Unified Communications Manager**, page 274 (required)
- **Configuring SRST Fallback on Cisco Unified Communications Manager**, page 275 (required)
- **Configuring CAPF on Cisco Unified Communications Manager**, page 277 (required)

#### Adding an SRST Reference to Cisco Unified Communications Manager

The following procedure describes how to add an SRST reference to Cisco Unified Communications Manager:

Before following this procedure, verify that credentials service is running in the Cisco Unified SRST Router.

To enable credentials service, see the “Enabling Credentials Service on the Secure Cisco Unified SRST Router” on page 264.
How to Configure Secure Unified SRST

For complete information on adding Cisco Unified SRST to Cisco Unified Communications Manager, see the “Survivable Remote Site Telephony Configuration” section for the Cisco Unified Communications Manager version that you are running. All Cisco Unified CM administration guides are at the following URL:

Step 1
In the menu bar in Cisco Unified Communications Manager, choose CCMAdmin > System > SRST.

Step 2
Click Add New SRST Reference.

Step 3
Enter the appropriate settings. Figure 9-3 shows the available fields in the SRST Reference Configuration window.

   a. Enter the name of the SRST gateway, the IP address, and the port.
   b. Check the box asking if the SRST gateway is secure.
   c. Enter the certificate provider (credentials service) port number. Credentials service runs on default port 2445.

Step 4
To add the new SRST reference, click Insert. The message “Status: Insert completed” displays.

Step 5
To add more SRST references, repeat Steps 2 to 4.

Configuring SRST Fallback on Cisco Unified Communications Manager

The following procedure describes how to configure SRST fallback on Cisco Unified Communications Manager by assigning the Unified SRST reference to a device pool.
For complete information about adding a device pool to Cisco Unified Communications Manager, see the “Device Pool Configuration” section in Cisco Unified Communications Manager Administration Guide for the Cisco Unified Communications Manager version that you are running. All Cisco Unified CM administration guides are at the following URL:

Step 1
In the menu bar in Cisco Unified Communications Manager, choose CCMAdmin > System > Device Pool.

Step 2
Use one of the following methods to add a device pool:

- If a device pool already exists with settings that are similar to the one that you want to add, choose the existing device pool to display its settings, click Copy, and modify the settings as needed. Continue with Step 4.
- To add a device pool without copying an existing one, continue with Step 3.

Step 3
In the upper, right corner of the window, click the Add New Device Pool link. The Device Pool Configuration window displays (see Figure 9-4).

Figure 9-4 Device Pool Configuration Window

Device Pool Configuration

Device Pool: Default (13 members*)

Status: Ready

Copy | Update | Delete | Reset Devices

Device Pool Settings

- Device Pool Name*
  - Default

- Cisco CallManager Group*
  - Default

- Date/Time Group*
  - CMLocal

- Region*
  - Default

- Softkey Template*
  - StandardUser

- SRST Reference*
  - jaso2031

- Calling Search Space for Auto-registration
  - NotSelected —

- Media Resource Group List
  - Disable

- Network Hold MOH Audio Source
  - jaso2031
  - SRST GW

- User Hold MOH Audio Source
  - < None >

- Network Locales
  - < None >

Step 4
Enter the SRST reference.

Step 5
Click Update to save the device pool information in the database.
Configuring CAPF on Cisco Unified Communications Manager

The Certificate Authority Proxy Function (CAPF) process allows supported devices, such as Cisco Unified IP Phones to request LSC certificates from the CAPF service on Cisco Unified Communications Manager. The CAPF utility generates a key pair and certificate that are specific for CAPF, and the utility copies this certificate to all Cisco Unified Communications Manager servers in the cluster.

For complete instructions on configuring CAPF in Cisco Unified Communications Manager, see the Cisco IP Phone Authentication and Encryption for Cisco Communications Manager documentation.

Enabling SRST Mode on the Secure Cisco Unified SRST Router

To configure secure SRST on the router to support the Cisco Unified IP Phone functions, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. call-manager-fallback
2. secondary-dialtone digit-string
3. transfer-system { blind | full-blind | full-consult | local-consult } 
4. ip source-address ip-address [ port port ]
5. max-ephones max-phones 
6. max-dn max-directory-numbers 
7. transfer-pattern transfer-pattern 
8. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> secondary-dialtone digit-string</td>
<td>Activates a secondary dial tone when a digit string is dialed.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# secondary-dialtone 9</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> transfer-system (blind</td>
<td>full-blind</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# transfer-system full-consult</td>
<td>- <strong>blind</strong>: Calls are transferred without consultation with a single phone line using the Cisco proprietary method.</td>
</tr>
<tr>
<td></td>
<td>- <strong>full-blind</strong>: Calls are transferred without consultation using H.450.2 standard methods.</td>
</tr>
<tr>
<td></td>
<td>- <strong>full-consult</strong>: Calls are transferred with consultation using a second phone line if available. The calls fallback to <strong>full-blind</strong> if the second line is unavailable.</td>
</tr>
<tr>
<td></td>
<td>- <strong>local-consult</strong>: Calls are transferred with local consultation using a second phone line if available. The calls fallback to <strong>blind</strong> for nonlocal consultation or nonlocal transfer target.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip source-address ip-address [port port]</td>
<td>Enables the router to receive messages from the Cisco IP Phones through the specified IP addresses and provides for strict IP address verification. The default port number is 2000.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> max-ephones max-phones</td>
<td>Configures the maximum number of Cisco IP phones that can be supported by the router. The maximum number is platform dependent. The default is 0. See the “Platform and Memory Support” section on page 25 for further details.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-ephones 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> max-dn max-directory-numbers</td>
<td>Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-dn 30</td>
<td>- <strong>max-directory-numbers</strong>: Maximum number of directory numbers or virtual voice ports supported by the router. The maximum number is platform dependent. The default is 0. See the “Platform and Memory Support” section on page 25 for further details.</td>
</tr>
</tbody>
</table>
How to Configure Secure Unified SRST

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7 transfer-pattern</td>
<td>Allows transfer of phone calls by Cisco Unified IP Phones to specified phone number patterns.</td>
</tr>
<tr>
<td>Example: Router(config-cm-fallback)# transfer-pattern .....</td>
<td>• transfer-pattern: String of digits for permitted call transfers. Wildcards are allowed.</td>
</tr>
<tr>
<td>Step 8 exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example enables SRST mode on your router:

```plaintext
Router(config)# call-manager-fallback
Router(config-cm-fallback)# secondary-dialtone 9
Router(config-cm-fallback)# transfer-system full-consult
Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000
Router(config-cm-fallback)# max-ephones 15
Router(config-cm-fallback)# max-dn 30
Router(config-cm-fallback)# transfer-pattern ......
Router(config-cm-fallback)# exit
```

Configuring Secure SCCP SRST

- Prerequisites for Configuring Secure SCCP SRST, page 279
- Restrictions for Configuring Secure SCCP SRST, page 279
- Verifying Phone Status and Registrations, page 280 (required)
- Configuration Examples for Secure SCCP SRST, page 287

Prerequisites for Configuring Secure SCCP SRST

- Cisco Unified Communications Manager 4.1(2) or later must be installed and must support security mode (authenticate and encryption mode).
- Unified SRST 12.3 or later releases for Secure SCCP support on Cisco 4000 Series Integrated Services Routers and Cisco Analog Voice Gateways mentioned in the section Secure SCCP SRST for Analog Voice Gateways, page 243. The configuration and behavior of Secure SCCP SRST fallback aligns with the existing support offered on Cisco Integrated Services Router Generation 2, unless specified otherwise.

Restrictions for Configuring Secure SCCP SRST

Not Supported in Secure SCCP SRST Mode (For Unified SRST 12.2 and prior releases)

- Cisco Unified Communications Manager versions before 4.1(2).
- Secure MOH; MOH stays active, but reverts to non-secure.
- Secure transcoding or conferencing.
How to Configure Secure Unified SRST

- Secure H.323 or SIP trunks.
- SIP phones interoperability.
- **Hot Standby Routing Protocol** (HSRP).

**Not Supported in Secure SCCP SRST Mode (For Unified SRST 12.3 and later releases)**
For information on the restrictions for Secure SCCP SRST support introduced on Unified SRST 12.3, see the section SCCP SRST in Restrictions for Configuring Secure SRST, page 240.

**Supported Calls in Secure SCCP SRST Mode (For Unified SRST 12.2 and prior releases)**
Only voice calls are supported in secure SCCP SRST mode. Specifically, the following voice calls are supported:

- Basic call
- Call transfer (consult and blind)
- Call forward (busy, no-answer, all)
- Shared line (IP phones)
- Hold and resume

For information on the features supported on Unified SRST 12.3 and later releases, see Feature Support for Secure SRST (SCCP), Unified SRST Release 12.3, page 246.

**Verifying Phone Status and Registrations**
To verify or troubleshoot Cisco Unified IP Phone status and registration, complete the following steps beginning in privileged EXEC mode.

**Note**
You can verify Phone Status and Registrations in secure SCCP SRST after you have performed the following steps:

- **Enabling Credentials Service on the Secure Cisco Unified SRST Router**, page 264
- **Adding an SRST Reference to Cisco Unified Communications Manager**, page 274
- **Enabling SRST Mode on the Secure Cisco Unified SRST Router**, page 277

**SUMMARY STEPS**

1. show ephone
2. show ephone offhook
3. show voice call status
4. debug ephone register
5. debug ephone state
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ephone</td>
<td>Use this command to display registered Cisco Unified IP Phones and their capabilities. The show ephone command also displays authentication and encryption status when used for secure SCCP SRST. In this example, authentication and encryption status is active with a TLS connection.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router# show ephone

ephone-1 Mac:1000.1111.0002 TCP socket:[5]  
activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32626 7970 keepalive 390 max_line 8  
button 1: dn 14 number 2002 CM Fallback CH1 IDLE

ephone-2 Mac:1000.1111.000B TCP socket:[12]  
activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32718 7970 keepalive 390 max_line 8  
button 1: dn 21 number 2011 CM Fallback CH1 IDLE

ephone-3 Mac:1000.1111.000A TCP socket:[16]  
activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32862 7970 keepalive 390 max_line 8  
button 1: dn 2 number 2010 CM Fallback CH1 IDLE
```

| **Step 2** show ephone offhook | Use this command to display Cisco IP Phone status and quality for all phones that are off hook. In this example, authentication and encryption status is active with a TLS connection, and there is an active secure call. |

**Example:**

```bash
Router# show ephone offhook

ephone-1 Mac:1000.1111.0002 TCP socket:[5]  
activeLine:1 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:1 offhook:1 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32626 7970 keepalive 391 max_line 8  
button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED  
Active Secure Call on DN 14 chan 1 :2002 10.1.1.40  
29632 to 10.1.1.40 25616 via 10.1.1.40  
G711Ulaw64k 160 bytes no vad  
Tx Pkts 295 bytes 49658 Rx Pkts 277 bytes 46531 Lost 0  
Jitter 0 Latency 0 callingDn 22 calledDn -1

ephone-2 Mac:1000.1111.000B TCP socket:[12]  
activeLine:1 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:1 offhook:1 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32718 7970 keepalive 391 max_line 8
```

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ephone</td>
<td>Use this command to display registered Cisco Unified IP Phones and their capabilities. The show ephone command also displays authentication and encryption status when used for secure SCCP SRST. In this example, authentication and encryption status is active with a TLS connection.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router# show ephone

ephone-1 Mac:1000.1111.0002 TCP socket:[5]  
activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32626 7970 keepalive 390 max_line 8  
button 1: dn 14 number 2002 CM Fallback CH1 IDLE

ephone-2 Mac:1000.1111.000B TCP socket:[12]  
activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32718 7970 keepalive 390 max_line 8  
button 1: dn 21 number 2011 CM Fallback CH1 IDLE

ephone-3 Mac:1000.1111.000A TCP socket:[16]  
activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32862 7970 keepalive 390 max_line 8  
button 1: dn 2 number 2010 CM Fallback CH1 IDLE
```

| **Step 2** show ephone offhook | Use this command to display Cisco IP Phone status and quality for all phones that are off hook. In this example, authentication and encryption status is active with a TLS connection, and there is an active secure call. |

**Example:**

```bash
Router# show ephone offhook

ephone-1 Mac:1000.1111.0002 TCP socket:[5]  
activeLine:1 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:1 offhook:1 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32626 7970 keepalive 391 max_line 8  
button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED  
Active Secure Call on DN 14 chan 1 :2002 10.1.1.40  
29632 to 10.1.1.40 25616 via 10.1.1.40  
G711Ulaw64k 160 bytes no vad  
Tx Pkts 295 bytes 49658 Rx Pkts 277 bytes 46531 Lost 0  
Jitter 0 Latency 0 callingDn 22 calledDn -1

ephone-2 Mac:1000.1111.000B TCP socket:[12]  
activeLine:1 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:1 offhook:1 ringing:0 reset:0  
reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32718 7970 keepalive 391 max_line 8
```
### Command or Action

- **button 1: dn 21 number 2011 CM Fallback CH1**
- **CONNECTED**
- **Active Secure Call on DN 21 chan 1 :2011 10.1.1.40 16382 to 10.1.1.40 16382 via 10.1.1.40**
- **G711Ulaw64k 160 bytes no vad**
- **Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0**
- **Jitter 0 Latency 0 callingDn -1 calledDn 11**

### Purpose
Step 3

show voice call status

Example:
CallID CID ccVdb Port DSP/Ch Called # Codec
0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw
0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw
0x1166 2C01 0x861D43D8 50/0/21.0 2012 g711ulaw
0x1167 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw
0x1168 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw
0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw
0x116A 2C07 0x86039700 50/0/2.0 *2010 g711ulaw
0x116B 2C07 0x860A374C 50/0/12.0 2010 g711ulaw
0x116C 2C0A 0x86119520 50/0/26.0 2016 g711ulaw
0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw
0x116E 2C0D 0x8608DC20 50/0/10.0 2022 g711ulaw
0x116F 2C0D 0x86039700 50/0/2.0 *2010 g711ulaw
0x1170 2C10 0x861398F0 50/0/23.0 2034 g711ulaw
0x1171 2C10 0x860CE3C0 50/0/16.0 2004 g711ulaw
0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw
0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw
0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw
0x1175 2C16 0x86164F48 50/0/30.0 *2026 g711ulaw
0x1176 2C19 0x860D8C64 50/0/17.0 2032 g711ulaw
0x1177 2C19 0x86063990 50/0/6.0 2006 g711ulaw
0x1178 2C1C 0x860B8894 50/0/14.0 *2002 g711ulaw
0x1179 2C1C 0x860EE8AC 50/0/19.0 *2004 g711ulaw
0x117A 2C1F 0x86043FA4 50/0/3.0 2008 g711ulaw
0x117B 2C1F 0x861247A8 50/0/24.0 *2008 g711ulaw
0x117C 2C22 0x8608337C 50/0/9.0 2020 g711ulaw
0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw
0x117E 2C25 0x86063990 50/0/6.0 2006 g711ulaw

Use this command to show the call status for all voice ports on the Cisco Unified SRST router. This command is not applicable for calls between two POTS dial peers.
Chapter 9      Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

Step 4  debug ephone register

Example:
Router# debug ephone register
EPHONE registration debugging is enabled
*Jun 29 09:16:02.180: New Skinny socket accepted [2] (0 active)
*Jun 29 09:16:02.180: sin_family 2, sin_port 51617, in_addr 10.5.43.177
*Jun 29 09:16:02.180: skinny_socket_process: secure skinny sessions = 1
*Jun 29 09:16:02.180: add_skinny_secure_socket: pid =155, new_sock=0, ip address = 10.5.43.177
*Jun 29 09:16:02.180: skinny_secure_handshake: pid =155, sock=0, args->pid=155, ip address = 10.5.43.177
*Jun 29 09:16:02.184: Start TLS Handshake 0 10.5.43.177 51617
*Jun 29 09:16:02.184: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:03.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:04.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:05.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:06.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:07.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:08.188: CRYPTO_PKI_OPSSL - Verifying 1 Certs
*Jun 29 09:16:08.212: TLS Handshake completes

Use this command to debug the process of Cisco IP phone registration.
### Command or Action

debug ephone state

### Purpose

Use this command to review call setup between two secure Cisco Unified IP Phones. The debug ephone state trace shows the generation and distribution of encryption and decryption keys between the two phones.

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ephone state</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Router# debug ephone state
*Jan 11 18:33:09.231:%SYS-5-CONFIG_I:Configured from console by console
*Jan 11 18:33:11.747:ephone-2[2]:--SkinnySyncPhoneDnOverlay is onhook
*Jan 11 18:33:11.747:ephone-2[2]:SIEZE on activeLine 0 activeChan 1
*Jan 11 18:33:11.747:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsOffHook
*Jan 11 18:33:11.747:ephone-2[2]:Check Plar Number
*Jan 11 18:33:11.751:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:11.751:dn_tone_control DN=2 chan 1 tonetype=33:DtoInsideDialTone onoff=1 pid=232
*Jan 11 18:33:15.031:dn_tone_control DN=2 chan 1 tonetype=0:DtoSilence onoff=0 pid=232
*Jan 11 18:33:16.039:ephone-2[2]:Skinny-to-Skinny call DN 2 chan 1 to DN 4 chan 1 instance 1
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsProceed
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsRingOut
*Jan 11 18:33:16.039:ephone-2[2]:callingNumber 6000
*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 1 called 6001 calling 6000 origcalled
*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000 origcalled 6001 calltype 2
*Jan 11 18:33:16.039:ephone-2[2]:Call Info for chan 1
*Jan 11 18:33:16.039:ephone-2[2]:Original Called Name 6001
*Jan 11 18:33:16.039:ephone-2[2]:6000 calling
*Jan 11 18:33:16.047:ephone-3[3]:SetCallState line 1 DN 4(4) chan 1 ref 7 TsRingIn
*Jan 11 18:33:16.047:ephone-3[3]:callingNumber 6000
*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 7 called 6001 calling 6000 origcalled
*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000 origcalled 6001 calltype 1
*Jan 11 18:33:16.047:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:16.047:ephone-3[3]:Original Called Name 6001
*Jan 11 18:33:16.047:ephone-3[3]:6000 calling
*Jan 11 18:33:16.047:ephone-3[3]:6001
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 11 18:33:16.051:dn_tone_control DN=2 chan 1 tonetype=36:DtAlertingTone onoff=1 pid=232</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:OFFHOOK</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:SkinnySyncPhoneDnOverlay is onhook</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:Ringer Off</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:ANSWER call</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsOffHook</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3][SEP000DEDAB3EBF]:Answer</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsConnected</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-2[2]:callingNumber 6000</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-2[2]:Call Info DN 4 line 1 ref 7 call state 4 called 6001 calling 6000 origcalled</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.831:ephone-3[3]:Call Info DN 4 line 1 ref 7 calling 6001 calling 6001 origcalled</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Call Info for chan 1</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Original Called Name 6001</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:6000 calling</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-2[2]:OpenReceive DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:Security Key Generation</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:20.835:ephone-3[3]:OpenReceive DN 4 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:21.087:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232</td>
<td></td>
</tr>
<tr>
<td>Jan 11 18:33:21.095:ephone-2[2]:OpenReceiveChannelAck:IP 1.1.1.8, port=25552, dn_index=2, dn=2, chan=1</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 9      Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

Configuration Examples for Secure SCCP SRST

This section provides the following configuration examples:

- Secure SCCP SRST: Example, page 287
- Control Plane Policing: Example, page 292

Note

IP addresses and hostnames in examples are fictitious.

Secure SCCP SRST: Example

This section provides a configuration example to match the identified configuration tasks in the previous sections. This example does not include using a third-party CA; it assumes the use of the Cisco IOS certificate server to generate your certificates.

Router# show running-config

```
! Define Unified Communications Manager.
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.1.1.13
ccm-manager config
```
How to Configure Secure Unified SRST

! Define root CA.
crypto pki server srstcaserver
database level complete
database url nvram
issuer-name CN=srstcaserver

! Define CTL/7970 trustpoint.
crypto pki trustpoint 7970
enrollment terminal
revocation-check none

! Define CAPF/7960 trustpoint.
crypto pki trustpoint 7960
enrollment terminal
revocation-check none

! SRST router device certificate.
crypto pki certificate chain srstcaserver
certificate 02
308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301B170D 303443034
31323133 35323233 5A170D30 35303431 32313935 32323335 30343132 300F0603
55404513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
32363931 26363973 636F2E63 6F6D0305 300D0609 2A864886 F70D0101 01050003
4B030348 0214000D 0CC354F8 5F7C1AE7 7A2535F2 056E0485 22896D36 6A7C091
C9F8F9AB AE9D1F9B D4B7A67 F1251174 193BB1A3 12946123 E5C1CCD7 A2B6155
FA2ED743 3FBBB902 03100001 A330302E 300B0603 551D0F04 04030205 A0310F06
05551D23 04183016 8014F829 CB97AD60 18D05467 FC293963 C2470691 9FBD030D
06092A86 4886F70D 01010405 00038181 007EB48E CAEB1E13 D17A1A85 D7F0D665
CB841B78 1151BD78 B339763 59EC650E 49371F6D 99CB2D67 E88DF9D 9E43A5F2
FB2B13A0 3A4F656A 11239473 41478AFC A86ED5A1 AC518E0B 8657CEBB ED2BDE8E
B586FE67 0CC358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6EC29EE7 08BC2752
C3AF4A66 BD007348 D013000A EA3C206D CF quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301B170D 303443034
31323133 35323233 5A170D30 35303431 32313935 32323335 30343132 300F0603
55404513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
32363931 26363973 636F2E63 6F6D0305 300D0609 2A864886 F70D0101 01050003
4B030348 0214000D 0CC354F8 5F7C1AE7 7A2535F2 056E0485 22896D36 6A7C091
C9F8F9AB AE9D1F9B D4B7A67 F1251174 193BB1A3 12946123 E5C1CCD7 A2B6155
FA2ED743 3FBBB902 03100001 A330302E 300B0603 551D0F04 04030205 A0310F06
05551D23 04183016 8014F829 CB97AD60 18D05467 FC293963 C2470691 9FBD030D
06092A86 4886F70D 01010405 00038181 007EB48E CAEB1E13 D17A1A85 D7F0D665
CB841B78 1151BD78 B339763 59EC650E 49371F6D 99CB2D67 E88DF9D 9E43A5F2
FB2B13A0 3A4F656A 11239473 41478AFC A86ED5A1 AC518E0B 8657CEBB ED2BDE8E
B586FE67 0CC358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6EC29EE7 08BC2752
C3AF4A66 BD007348 D013000A EA3C206D CF quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301B170D 303433034
31323133 35323233 5A170D30 35303431 32313934 3531365A 30173115 30130630
55404513 08437273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818DD003 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
10519DF8 32A91B3 3C363635 74691934 9E765B1 059E24B6 32154E99 105C9A99
9619993F CC725C25 73570EBA E6335A12 2AA9F991 99325BFD 9BB35EEB C10F8963
9D8FC222 EEBAC831 71ACD3A7 4EB18AEF D5775159 76F8F499 5AD0849D CAA41147
DDL866020 2185D503 C3704288 0F93B203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0D01 01FF0404 03001816 301D0603 551D0E04
16041F9B 29CB97AD 6019D054 678FC939 63C24706 91F9B603 1D020418
30168014 F829CE97 AD60180D 5467FC29 3961C247 0691F9B3 000D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DF0D3A DBD1338F 6792C805
47A81B19 795B8AA5 035400DB F859DABF 21892B5B E71A8283 089B0414 860388B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
How to Configure Secure Unified SRST

crypto pki certificate chain srstcaserver

quit

crypto pki certificate chain PEM

Certificate chain PEM:

Certificate:

BEGIN CERTIFICATE

[Certificate Data]

END CERTIFICATE

Certificate:

BEGIN CERTIFICATE

[Certificate Data]

END CERTIFICATE

Certificate:

BEGIN CERTIFICATE

[Certificate Data]

END CERTIFICATE

quit
Chapter 9 Configuring Secure SRST for SCCP and SIP

How to Configure Secure Unified SRST

```plaintext
quit

crypto pki certificate chain 7960
certificate ca F301
30820100 30820160 A0302021 020202F3 01300D06 092A6846 86F7D001 01050500
30413108 30090603 55040613 02555331 1A301806 0355540A 13114369 73636F20
53797374 56E7320 496E6331 16301406 03555004 13034341 50462D33 35453038
33333323 1E170D30 34303430 39230325 35303235 37003319 30343036 32033535
3015A3A3 41310B30 09060355 04061302 5553311A 0180603 55040A13 11436973
636F2053 7977346B 536B3249 6E633116 30140603 55040A13 01343150 462D3335
45030383 33323081 9F300D06 092A6846 86F7D001 01050500 03818D00 30819802
811100CA BD9B6035 366B44E6 0F693A47 250F8F65 D76C35F7 89BC14FD 1D122CE0
F585CDD5 AA87EF6F 41AD936F E5C93163 3B55311A AF82A5F6 D663E21C EB89EEBA
F5271423 C38E87DC E0B37097 6E1AAB4F D3823B12 53547480 23BA1A90 295179B6
85A0E8B3 77D00D33 B9710A88 890CD4D DB55ADD0 964369BA 489043B6 B667E60F
9359FAB2 03010001 09060403 0255540A 13034341 50462D33 35453038
6F98D2AD 40C309E2 C5B8841C 5189271F 018D64E8 98BEC665 2AFFCC28 54078A4B
8F7772C7 E0347A6C 2626F50B B36A6174 B68C1D78 C228FEA8 A89C9EF8 CBBAA9F6
0F30E151 431670F9 198514D9 808D1235 18137F1E 50D5D32E 1D29C927 95EF4096
421AF22F 5C1D5804 B83F38EE 95B044F5 86563BEF DF97F65B CB490A

quit
!
no crypto isakmp enable
!
! Enable IPSec.
crypto isakmp policy 1
authentication pre-share
lifetime 28800
crypto isakmp key cisco123 address 10.1.1.13
! The crypto key should match the key configured on Cisco Unified Communications Manager.
! The crypto IPSec configuration should match your Cisco Unified Communications Manager configuration.
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 10.1.1.13
set transform-set rtpset
```
match address 116
!
!
interface FastEthernet0/0
ip address 10.1.1.22 255.255.255.0
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
!
! Define traffic to be encrypted by IPSec.
access-list 116 permit ip host 10.1.1.22 host 10.1.1.13
!
control-plane
!
!
call application alternate DEFAULT
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/0/2
!
voice-port 1/0/3
!
voice-port 1/1/0
timing hookflash-out 50
!
voice-port 1/1/1
!
voice-port 1/1/2
!
voice-port 1/1/3
!
!
! Enable MGCP voice protocol.
mgcp
mgcp call-agent 10.1.1.13 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
!
dial-peer voice 81235 pots
  application mgcpapp
  destination-pattern 81235
  port 1/1/0
  forward-digits all
!

dial-peer voice 81234 pots
  application mgcpapp
  destination-pattern 81234
  port 1/0/0
!
dial-peer voice 999100 pots
  application mgcpapp
  port 1/0/0
!
dial-peer voice 999110 pots
  application mgcpapp
  port 1/1/0
!
!
! Enable credentials service on the gateway.
credentials
  ip source-address 10.1.1.22 port 2445
  trustpoint srstca
!
!
! Enable SRST mode.
call-manager-fallback
  transport-tcp-tls
  secondary-dialtone 9
  transfer-system full-consult
  ip source-address 10.1.1.22 port 2000
  max-ephones 15
  max-dn 30
  transfer-pattern ......
.
.

Control Plane Policing: Example

This section provides a configuration example for the security best practice of protecting the credentials service port using control plane policing. Control plane policing protects the gateway and maintains packet forwarding and protocol states despite a heavy traffic load. For more information on control planes, see the Control Plane Policing documentation.

Router# show running-config
.
.
.
! Allow trusted host traffic.
access-list 140 deny tcp host 10.1.1.11 any eq 2445

! Rate-limit all other traffic.
access-list 140 permit tcp any any eq 2445
access-list 140 deny ip any any

! Define class-map "sccp-class."
class-map match-all sccp-class
match access-group 140

policy-map control-plane-policy
class sccp-class
police 8000 1500 1500 conform-action drop exceed-action drop
! Define aggregate control plane service for the active Route Processor.
control-plane
service-policy input control-plane-policy

Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST

Cisco Unified Survivable Remote Site Telephony (Cisco SRST) provides secure call signaling and Secure Real-time Transport Protocol (SRTP) for media encryption to establish a secure, encrypted connection between Cisco Unified IP Phones and gateway devices.

- Prerequisites for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293
- Restrictions for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST, page 293
- Information About Cisco Unified SIP SRST Support of Secure SIP Signaling and SRTP Media, page 294
- Configuring Cisco Unified Communications Manager, page 294
- Configuring Phones, page 295
- Configuring SIP options for Secure SIP SRST, page 296
- Configuring SIP SRST Security Policy, page 297 (optional)
- Configuring SIP User Agent for Secure SIP SRST, page 298 (optional)
- Verifying the Configuration, page 300
- Configuration Example for Cisco Unified SIP SRST, page 302

Prerequisites for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST

- Cisco IOS Release 15.0(1)XA and later releases.
- Cisco Unified IP Phone firmware release 8.5(3) or later.
- Complete the prerequisites and necessary tasks found in Prerequisites for Configuring SIP SRST Features Using Back-to-Back User Agent Mode.
- Prepare the Cisco Unified SIP SRST device to use certificates as documented in Preparing the Cisco Unified SRST Router for Secure Communication.

Restrictions for Configuring Secure SIP Call Signaling and SRTP Media with Cisco SRST

SIP phones may be configured on the Cisco Unified CM with an authenticated device security mode. The Cisco Unified CM ensures integrity and authentication for the phone using a TLS connection with NULL-SHA cipher for signaling. If an authenticated SIP phone fails over to the Cisco Unified SRST device, it will register using TCP instead of TLS/TCP, thus disabling the authenticated mode until the phone fails back to the Cisco Unified CM.

- By default, non-secure TCP SIP phones are permitted to register to the SRST device on failover from the primary call control. Support for TCP SIP phones requires the secure SRST configuration described in this section even if no encrypted phones are deployed. Without the secure SIP SRST configuration, TCP phones will register to the SRST device using UDP for signaling transport.
Information About Cisco Unified SIP SRST Support of Secure SIP Signaling and SRTP Media

Beginning with Cisco IP Phone firmware 8.5(3) and Cisco IOS Release 15.0(1)XA, Cisco SRST supports SIP signaling over UDP, TCP, and TLS connections, providing both RTP and SRTP media connections based on the security settings of the IP phone.

Cisco SRST SIP-to-SIP and SIP-to-PSTN support includes the following features:

- Basic calling
- Hold/resume
- Conference
- Transfer
- Blind transfer
- Call forward

Cisco SRST SIP-to-other (including SIP-to-SCCP) support includes basic calling, although other features may work.

Configuring Cisco Unified Communications Manager

Like SCCP-controlled devices, SIP-controlled devices will use the SRST Reference profile that is listed in their assigned Device Pool. The SRST Reference profile must have the "Is SRST Secure" check box selected if SIP/TLS communication is desired in the event of a WAN failure.

Note

All Cisco Unified IP Phones must have their firmware updated to version 8.5(3) or later. Devices with firmware earlier than 8.5(3) will need to have a separate Device Pool and SRST Reference profile created without the "Is SRST Secure" option selected; SIP-controlled devices in this Device Pool will use SIP over UDP to attempt to register to the SRST router.

In Cisco Unified CM Administration, under System > SRST:

- For the secure SRST profile, Is SRST Secure? must be checked. The SIP port must be 5061.
- For the non-secure SRST profile, the Is SRST Secure? checkbox should NOT be checked and the SIP port should be 5060.

Under Device > Phone:

- Secure phones must belong to the pool that uses the secure SRST profile.
- Non-secure phones must belong to the pool that uses the non-secure SRST profile.

Note

SIP phones will use the transport method assigned to them by their Phone Security Profile.
Configuring Phones

This section specifies that SRTP should be used to enable secure calls and allows non-secure calls to "fallback" to using RTP media.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. srtp
5. allow-connections sip to h323
6. allow-connections sip to sip
7. 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>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 srtp</td>
<td>Specifies that SRTP be used to enable secure calls.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# srtp</td>
<td></td>
</tr>
<tr>
<td>Step 5 allow-connections sip to h323</td>
<td>(Optional) Allows connections from SIP endpoints to H.323 endpoints.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# allow-connections sip to h323</td>
<td></td>
</tr>
<tr>
<td>Step 6 allow-connections sip to sip</td>
<td>Allows connections from SIP endpoints to SIP endpoints.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# allow-connections sip to sip</td>
<td></td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring SIP options for Secure SIP SRST

This section explains how to configure secure SIP SRTP.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. url sip | sips
6. srtp negotiate cisco
7. 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>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>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service configuration mode.</td>
</tr>
<tr>
<td>Example::</td>
<td>Router(config)# voice service voip</td>
</tr>
<tr>
<td>Step 4 sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voi-serv)# sip</td>
</tr>
<tr>
<td>Step 5 url sip</td>
<td>sips</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(conf-serv-sip)# url sips</td>
</tr>
<tr>
<td>Step 6 srtp negotiate cisco</td>
<td>Enables a Cisco IOS SIP gateway to negotiate the sending and accepting of RTP profiles in response to SRTP offers.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(conf-serv-sip)# srtp negotiate cisco</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(conf-serv-sip)# end</td>
</tr>
</tbody>
</table>

Configuring SIP SRST Security Policy

This section explains how to secure mode to block registration of non-secure phones to the SRST router.

SUMMARY STEPS

1. voice register global
2. security-policy secure | no security-policy
3. end
How to Configure Secure Unified SRST

![Image of page from the document]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 voice register global</td>
<td>Enter voice register global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# voice register global</td>
</tr>
<tr>
<td>Step 2 security-policy secure</td>
<td>Configure SIP registration security policy so that only SIP/TLS/TCP connections are allowed. For device-default mode, use the no security-policy command. Device-default mode allows non-secure devices to register without using TLS.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# security-policy secure</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>End the current configuration session and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# end</td>
</tr>
</tbody>
</table>

Configuring SIP User Agent for Secure SIP SRST

This section explains how the strict-cipher limits the allowed encryption algorithms.

SUMMARY STEPS

1. sip-ua
2. registrar ipv4:destination-address expires seconds
3. xfer target dial-peer
4. crypto signaling default trustpoint string [strict-cipher]
5. crypto signaling remote-addr ip address subnet mask trustpoint trustpoint-name
6. end
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> registrar ipv4:destination-address expires seconds</td>
<td>Enables the gateway to register E.164 telephone numbers with primary and secondary external SIP registrars. destination-address is the IP address of the primary SIP registrar server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sip-ua)# registrar ipv4:192.168.2.10 expires 3600</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> xfer target dial-peer</td>
<td>Specifies that SRST should use the dial-peer as a transfer target instead of what is in the message body.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sip-ua)# xfer target dial-peer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> crypto signaling default trustpoint string [strict-cipher]</td>
<td>Identifies the trustpoint string keyword and argument used during the TLS handshake. The trustpoint string keyword and argument refer to the gateway’s certificate generated as part of the enrollment process, using Cisco IOS public-key infrastructure (PKI) commands. The strict-cipher keyword restricts support to TLS RSA encryption with the Advanced Encryption Standard-128 (AES-128) cipher-block-chaining (CBC) Secure Hash Algorithm (SHA) (TLS_RSA_WITH_AES_128_CBC_SHA) cipher suite. To configure device-default mode, omit the strict-cipher keyword.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sip-ua)# crypto signaling default trustpoint 3745-SRST strict-cipher</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 5** crypto signaling remote-addr {ip address | subnet mask} trustpoint trustpoint-name | The trustpoint label refers to the CUBE’s certificate that is generated with the Cisco IOS PKI commands as part of the enrollment process. Keywords and arguments are as follows:  
- **remote-addr ip address**—Associates an IP address to a trustpoint.  
- **trustpoint trustpoint-name**—Refers to the SIP gateways certificate generated as part of the enrollment process using Cisco IOS PKI commands |
| **Example:** Router(config-sip-ua)# crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srst-trunk1 | |
| **Step 6** end | Ends the current configuration session and returns to privileged EXEC mode. |
| **Example:** Router(config-sip-ua)# end | |

### Multiple Trustpoints

Use the default trustpoint configuration under sip-ua config mode for phones registering to Unified SRST in secure mode. For example, srstca is the default trustpoint for Secure SRST. This default signaling trustpoint is used for all SIP TLS interactions from SIP phones to Unified Secure SRST router.
In a deployment scenario with multiple trustpoints, communication with a service provider over a secure trunk with certificate issued by CA is achieved using the CLI command `crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srsr-trunk1` under `sip-ua` config mode.

Example

The following example shows a sample configuration of multiple trustpoints for a Unified SRST deployment. In this example, the `srsr-trunk1` trustpoint points to the network with IP address `8.39.0.0`, and `srsr-trunk2` trustpoint points to the network with IP address `8.41.20.20`.

```plaintext
sip-ua
crypto signaling remote-addr 8.39.0.0 255.255.0.0 trustpoint srsr-trunk1
crypto signaling remote-addr 8.41.20.20 255.255.0.0 trustpoint srsr-trunk2
crypto signaling default trustpoint securest
```

Verifying the Configuration

The following examples show a sample configuration displayed by the `show sip-ua status registrar` command and the `show voice register global` command.

The `show sip-ua status registrar` command in privileged EXEC mode displays all SIP endpoints that are currently registered with the contact address.

```plaintext
Router# show sip-ua status registrar
 Line destination expires(sec) contact transport call-id peer
 =========== =============== ============ ===============
3029991 192.168.2.108 388 192.168.2.108 TLS 00120014-4ae40064-f1a3e9fe-8d3d0170219.168.2.1 40004
3029993 192.168.2.103 382 192.168.2.103 TCP 001bd433-1c840052-655cd596-4e992ed9193.168.2.1 40011
3029982 192.168.2.106 406 192.168.2.106 UDP 001d452c-dcbba0056-0481d321-1f3f848d9192.168.2.1 40001
3029983 192.168.2.106 406 192.168.2.106 UDP 001d452c-dcbba0057-1c69b699-d8de66259192.168.2.1 40003
3029992 192.168.2.107 414 192.168.2.107 TLS 001e7a25-50c9002c-48ef7663-50c717949192.168.2.1 40005
```

The `show voice register global` command in privileged EXEC mode displays all global configuration parameters associated with SIP phones.

```plaintext
Router# show voice register global
 CONFIG [Version=8.0]
 ===========
 Version 8.0
 Mode is srst
 Max-pool is 50
 Max-dn is 100
 Outbound-proxy is enabled and will use global configured value
 Security Policy: DEVICE-DEFAULT
 timeout interdigit 10
 network-locale[0] US (This is the default network locale for this box)
network-locale[1] US
 user-locale[0] US (This is the default user locale for this box)
```
How to Configure Secure Unified SRST

user-locale[1] US
user-locale[2] US
user-locale[3] US
user-locale[4] US
Router#
Configuration Example for Cisco Unified SIP SRST

Current configuration : 15343 bytes

! Last configuration change at 05:34:06 UTC Tue Jun 13 2017
! NVRAM config last updated at 11:57:03 UTC Thu Jun 8 2017
!
version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname router
!
boot-start-marker
boot-end-marker
!

vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
! card type command needed for slot/bay 0/3
no logging queue-limit
logging buffered 20000000
no logging rate-limit
no logging console
enable password xxxx
!
no aaa new-model
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki server SRST-CA-2
  database level complete
  no database archive
  grant auto
!
crypto pki trustpoint TRUSTPT-SRST-CA-2
  enrollment url http://10.0.0.1:80
  serial-number
  revocation-check none
  rsakeypair srstcakey 2048
  rsakeypair SRST-CA-2
!
crypto pki trustpoint SRST-CA-2
  revocation-check crl
  rsakeypair SRST-CA-2
!
crypto pki trustpoint Cisco_Manufacturing_CA
  enrollment terminal
  revocation-check none
!
crypto pki trustpoint CAPF-3a66269a
  enrollment terminal
  revocation-check none
crypto pki trustpoint Cisco_Root_CA_2048

enrollment terminal
revocation-check none

crypto pki certificate chain TRUSTPT-SRST-CA-2

certificate ca 01

quit
Section 9.4.2.1 - Configuring Secure SRST for SCCP and SIP

1. Open the Cisco Unified Secure SRST configuration tool.
2. Navigate to the Secure SRST configuration menu.
3. Select the SCCP and SIP service type.
4. Configure the following parameters:
   - Addressing Mode: SCCP
   - Message Center: SIP
5. Save the configuration changes.

Chapter 9 - Configuring Secure SRST for SCCP and SIP

Chapter 9 - Configuring Secure SRST for SCCP and SIP

Certificate:

- **Common Name:** Cisco_Manufacturing_CA
- **Subject:** 
  - **O:** Cisco Systems, Inc.
  - **OU:** Engineering
- **Serial Number:** 39804321420354321
- **Issuer:** Cisco Systems, Inc.

Certificate Authority:

- **Common Name:** Cisco_Manufacturing_CA
- **Subject:** 
  - **O:** Cisco Systems, Inc.
  - **OU:** Engineering
- **Serial Number:** 39804321420354321
- **Issuer:** Cisco Systems, Inc.

SSL Configuration:

- **Protocol:** SSLv3
- **Cipher Suite:** RC4-MD5-SHA
- **SSL Version:** 3.0
- **SSL Protocol:** TLSv1.2

Cisco Unified SCCP and SIP SRST System Administrator Guide

9-304
How to Configure Secure Unified SRST

0603551D 0F040403 0202A430 13060355 1D25040C 300A0608 2B060105 
005003B2 010100BF 0E040302 02010030 0D06092A 864886F7 0D01010B 
05000382 010100BF 0D0938F3 35710000 97AD876D B4015C21 300A1BD0 
041A844BD 597CD278 718A6431 BA94C024 7EC64BA0 13060355 1D25040C 
300A0608 2B060105 0D06092A 864886F7 0D01010B 005003B2 010100BF 
0E040302 02010030 0D06092A 864886F7 0D01010B 05000382 010100BF 
0D0938F3 35710000 97AD876D B4015C21 300A1BD0 041A844BD 597CD278 
718A6431 BA94C024 7EC64BA0 

quit

crypto pki certificate chain Cisco_Root_CA_2048

certificate ca 5F820343 3082022B A0030201 02010030 0D06092A 864886F7 0D010105 
05000382 0101009D 9D8484A3 41A97C77 0CB753CA 4E445062 EF547CD3 75171CE8 
7BA9AAAB 6ED21588 4859D0E6 FC83D0CC B98CE026 68704A7B DF21179E F46105C9 
15C8CF16 DA356189 943A3884 A8319878 99B94E6F 2C53126C CD31DA2B 24BB31C4 
2BF8F8344 6F863D24 7709E9AB 2A81F6A6 56F6200F 11549781 75A725CE 6792E86F 596A8265 
EBF7B8A7 E2BD758B 6F924B4F C1001A46 D405C66A 2BC58F58 60A51274 
8DF6947F CE1B70DE 701B2D66 6ECDA601 A83C12C2 A93A06EB 5EB8E620 B87A91E3 
B568E9A0 E7C40174 A853092B 4A906F65 120E824D 8E639DFE EB981ADB 53A61360 
APC727CD7 C76C1725 D473F3B4 65080180 944E1BFF A4EB1CDF 92E2DE05 DF021013 
A351304F 300B0603 551DF040 03030201 86300F06 3051D13 0101004F 05300310 
01FF301D 0603551D 0E040160 427F5C38 151E69EA 020916AD 2BA08960 5FDA7E8F 
AA301006 092B0601 0D010030 0D06092A 864886F7 0D010015 
050003B2 0101009D 9DBA4843 41A97C77 0CB753CA 4E445062 EF547CD3 75171CE8 
E0C6484B B6F6E43A 198156B0 6581E996 62A5A5A3 64C1646E 5433C677 FEC51BCA 
E65D25CA FSF0939A 83112E6C CBF78445 FFE87058B ABE7DBFC 4BE13784 DA89B97 
701EF0E2 8DB7BD8B 09DB169A 62A917B A9494F7E E86E95D8 83273CD5 68490ED4 
9DF62EBA A7E88310 AA2C1F44 FC95A3B3 06F7DB60 0ADEB48A 63B09CA9 F2A4B953 
0187D068 A4277FAB FF69FA9C 40388867 8439C684 65F7C953 DB98EE1E C0432F8F 
09B36EFFF 66C5FEEF 17B35812 2509145E E3C0DB14 B6ECF292 6F742AF2 812D592 
91E09E07 3C326805 8548DBF7 57E25121 931A549F 0570C04A 71601E43 0B601EFE 
A3CEB119 E10B35 

quit

voice service voip

no ip address trusted authenticate

media bulk-stats

media disable-detailed-stats

allow-connections sip to sip

srtp

no supplementary-service sip refer

supplementary-service media-renegotiate

no supplementary-service sip handle-replaces

fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none

sip registrar server expires max 120 min 60

voice register global

default mode

no allow-hash-in-dn

security-policy secure

max-dn 50

max-pool 40
voice register pool 1
  id network 10.0.0.1 mask 255.255.0.0
dtmf-relay rtp-nte
  codec g711ulaw
!
voice hunt-group 1 sequential
  final 89898
  list 1008,2005
  timeout 5
  pilot 1111
!
voice-card 0/1
  no watchdog
!
voice-card 0/2
  no watchdog
!
voice-card 0/3
  no watchdog
!
voice-card 1/0
  no watchdog
!
license udi pid ISR4451-X/K9 sn FOC174356SL
license accept end user agreement
license boot level uck9
license boot level securityk9
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
  mode none
!
interface GigabitEthernet0/0/0
  ip address 10.0.0.1 255.255.0.0
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/2
  ip address 10.0.0.1 255.0.0.0
  negotiation auto
!
interface GigabitEthernet0/0/3
  no ip address
  negotiation auto
!
interface Service-Engine0/1/0
  shutdown
!
interface Service-Engine0/2/0
  shutdown
!
interface Service-Engine0/3/0
!
interface Service-Engine1/0/0
!
interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  no ip address
negotiation auto
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
control-plane
!
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/2/0
!
voice-port 0/2/1
!
voice-port 0/2/2
!
voice-port 0/2/3
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
sip-ua
    crypto signaling default trustpoint TRUSTPT-SRST-CA-2
!
!
credentials
    ip source-address 10.0.0.1 port 2445
    trustpoint TRUSTPT-SRST-CA-2
!
!
call-manager-fallback
    max-conferences 8 gain -6
    transfer-system full-consult
    max-phones 50
    max-dn 50
    call-park system application
    fac standard
!
!
line con 0
    exec-timeout 0 0
    length 0
    transport input none
    stopbits 1
    line aux 0
    stopbits 1
    line vty 0 4
    exec-timeout 0 0
    password xxxx
    no login
    length 0
    transport preferred none
    transport input telnet ssh
Additional References

The following sections provide references related to this feature.
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS voice configuration</td>
<td>• <em>Cisco IOS Voice Configuration Library</em></td>
</tr>
<tr>
<td></td>
<td>• <em>Cisco IOS Voice Command Reference</em></td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>• Cisco Unified Communications Manager Documentation Guide for Release 8.0(2)</td>
</tr>
<tr>
<td>Documentation Guide for Release 8.0(2)</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified SRST configuration</td>
<td>• <em>Cisco Unified SRST and SIP SRST Command Reference</em></td>
</tr>
<tr>
<td>Cisco Unified SRST</td>
<td>• Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products</td>
</tr>
<tr>
<td>Cisco Unified Communications Operating</td>
<td>• Security</td>
</tr>
<tr>
<td>System Administration Guide, Release 6.1(1)</td>
<td></td>
</tr>
<tr>
<td>Configuring a Secure Survivable Remote</td>
<td>• Configuring a Secure Survivable Remote Site Telephony (SRST) Reference</td>
</tr>
<tr>
<td>Site Telephony (SRST) Reference</td>
<td></td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS 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>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</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/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>

Command Reference


- security-policy
- show voice register global
- show voice register all
Feature Information for Secure SCCP and SIP SRST

Table 9-4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS 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.

Note

Table 9-4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure SIP Call Signaling and SRTP Media with Cisco SRST</td>
<td>15.0(1)XA</td>
<td>Adds Session Initiation Protocol/Transport Layer Security/Transmission Control Protocol (SIP/TLS/TCP) support for secure call signaling and Secure Real-time Transport Protocol (SRTP) for media encryption to establish a secure, encrypted connection between Cisco Unified IP Phones and a failover device using Cisco Unified Survivable Remote Site Telephony (Cisco SRST). The following commands were introduced or modified: security-policy, show voice register global, show voice register all</td>
</tr>
</tbody>
</table>

Where to Go Next

If you require voicemail, see the voice-mail configuration instructions in the “Integrating Voicemail with Cisco Unified SRST” section on page 331.

For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
Configuring SIP Trunking on Unified SRST

This chapter describes how to configure SIP trunking on Cisco Unified Survivable Remote Site Telephony (Unified SRST).

Contents

This chapter describes the configuration recommendations and details on the various line side and SIP trunking features on Unified SRST. Also, details are provided on the co-location of Unified Border Element and Unified SRST.

- Unified SRST and Unified Border Element Co-location, page 313
- Configuration Recommendations for Unified SRST and Unified Border Element Co-location, page 315

Unified SRST and Unified Border Element Co-location

For Unified SRST Release 12.1 and later releases, you can deploy product instances of Cisco Unified Border Element and Unified SRST (only for SIP) on the same Cisco 4000 Series Integrated Services Router. Co-location of Unified SRST and Unified Border element is supported from the release Cisco IOS XE Fuji 16.7.1. All the Cisco SIP IP Phones are supported for this deployment. The phone support includes, but is not limited to:

- Cisco IP Phone 7800 Series
- Cisco IP Phone 8800 Series
- Cisco Unified IP Phone 9900 Series

When the Wide Area Network (WAN) is available, the router acts as a pure Cisco Unified Border Element, and not as a Unified SRST.

During a WAN outage, the phones registered to the Unified Communications Manager fall back on the Unified SRST. However, phones registered to Unified SRST can place or receive PSTN calls through SIP trunk.

The Unified SRST and the Unified Border Element feature set is limited to the features mentioned. The following features are supported on the phone when registered to Unified SRST:

- Incoming or Outgoing Basic Call
- Hold/Resume
- Call Forward
- Call Transfer
- Conference (Built-in Bridge)
- Hunt Groups
- MOH (for SIP lines in SRST mode)

The list of SIP trunk features supported for Unified SRST and Unified Border Element co-location are:

- SIP-UA Registration/Authentication, Registrar, Register/Register Refresh
- SIP-Server, Outbound Proxy
- DNS Service Record
- Bind Global / Dial-peer
- SRTP / TLS, SRTP – RTP Interworking
- Connection Reuse
- IP Trust List
- Voice class tenant
- RTP-NTE DTMF
- P-Called-Party ID, Privacy Header (PAI)
- SIP Normalization

For more information on configuring tenants on SIP trunks, see Cisco Unified Border Element Configuration Guide. For more information on the recommended configurations for the Unified Border Element co-location, see Configuration Recommendations for Unified SRST and Unified Border Element Co-location, page 315.

Figure 10-1 shows a co-located deployment of Unified SRST with Cisco Unified Border Element.

Figure 10-1  Co-located Deployment of Unified SRST and Cisco Unified Border Element
Configuration Recommendations for Unified SRST and Unified Border Element Co-location

The dial-peers created after the phones (registered to Unified Communications Manager) fall back on Unified SRST are dynamic dial-peers. Hence, the configurations under `voice service voip` and `sip-ua` are inherited by these dynamic dial-peers. Move `voice service voip` and `sip-ua` configurations under `voice class tenant` configuration mode to avoid configuration conflict. The `voice class tenant` is included in the SIP trunk dial-peer configuration.

Similarly, the relevant global configurations are grouped under a `voice class tenant` and can be applied on the dial-peer toward Unified Communications Manager as well. These configurations grouped under the `voice class tenant` are used whenever the Unified Communications Manager is available (WAN is available). For sample configurations of the co-located deployment of Unified SRST and Unified Border Element, see Examples, page 318.

The following are the configuration recommendations for the Unified SRST and Unified Border Element co-location:

- Move SIP trunk specific `voice service voip` and `sip-ua` configurations under `voice class tenant`. This is to avoid configuration conflict between SIP trunk and line side dial-peer configurations. When tenant is configured under dial-peer, the configurations are applied in the following order of preference:
  - Dial-peer configuration
  - Tenant configuration
  - Global configuration
Chapter 10    Configuring SIP Trunking on Unified SRST

Unified SRST and Unified Border Element Co-location

Note

Certain CLI commands which need to be moved under tenant, are moved under dial-peer configuration mode. This is because these CLIs are not available under voice class tenant. For example, the CLI command srtp fallback needs to be configured under dial-peer, not voice class tenant configuration mode.

• Use dial-peer groups feature to group multiple outbound dial-peers into a dial-peer group and configure this dial-peer group as the destination of an inbound dial-peer (Unified CM trunk). For more information on dial-peer groups, see Dial Peer Configuration Guide.

• Configure SIP Options Request Keepalives to monitor reachability towards Unified Communications Manager. For example:

  voice class sip-options-keepalive 101
  up-interval 30
  retry 3
  transport tcp

  Options keepalive under dialpeer

  dial-peer voice 101 voip
  description **CUCM/PBX**
  voice-class sip options-keepalive profile 101

• The relevant CLI commands for configuring dial-peer groups are:
  – voice class dpg dial-peer-group-id (Creates a dial-peer group.)
  – destination dpg dial-peer-group-id (Specifies the dial-peer group from which the outbound dial-peer(s) is chosen.)

• Avoid configuring dial-peer groups on the SIP trunk dial-peer pointing to the Service Provider router.

• Configure the destination pattern (.T) on the dial-peer that points to Unified Communications Manager.

• It is mandatory to configure voice class tenant on the dial-peers pointing towards the Service Provider router. A configuration with voice class tenant on the dial-peer pointing towards Unified Communications Manager is also validated, though it is not mandatory.

• Configure the CLI command destination dpg dial-peer-group-id (destination dpg 101) on the dial-peer pointing to inbound dial-peer for Unified Communications Manager SIP trunk. This dpg configuration has dial-peer information pointing to the Service Provider. You can configure preferences for the dial-peers within the dial-peer group:

  voice class dpg 1
  dial-peer 2900 preference 2
  dial-peer 3900 preference 1

• Do not configure incoming called-number (.T), from the dial-peer towards the Service Provider. Match the incoming call from SIP trunk using the dial-peer address information ‘From URI’, after removing incoming called-number (.T).

  voice class uri 201 sip
  host dns:sip-trunk.sample

  Under dial-peer:
  incoming uri from 201

• Configure the CLI command transport tcp tls v1.2 under sip-ua configuration mode, not voice class tenant.
Avoid modification of contact header in a Secure SIP to SIP (and vice versa) call flow, as it leads to call establishment issues. If sip-profiles are used to modify header information from sips: to sip: in SIP REQUESTS and RESPONSES, there must be rules to include ‘transport=tls’ in the contact header.

If dial-peers are using voice class codec, configure the same voice class codec under voice register pool too.

Ensure that an srtp voice-class is created using the voice class srtp-crypto crypto-tag command. A sample configuration is as follows:

```plaintext
voice class srtp-crypto 1
crypto 1 AES_CM_128_HMAC_SHA1_32
crypto 2 AES_CM_128_HMAC_SHA1_80
```

Configure the SIP Registrar under voice service voip sip configuration mode with maximum and minimum expiry time for an incoming registration using the CLI command registrar server [expires [max sec] [min sec]].

```
– registrar server expires max 120 min 60
```

Move all the CLI commands related to SIP Bind feature under voice class tenant configuration mode. For example, it is recommended to have the CLI commands voice-class sip bind control, and voice-class sip bind media, under voice class tenant configuration mode.

Exclude SIP ports from NAT services, if NAT is configured on the router. The recommended CLIs for excluding SIP ports from NAT services are:

```
– no ip nat service sip udp port 5060
– no ip nat service sip tcp port 5060
```

Configure the CLI commands no supplementary-service sip refer, no supplementary-service sip moved-temporarily, supplementary-service media-renegotiate under voice service voip configuration mode.

For the co-located deployment of Unified SRST and Unified Border Element, do not configure the CLI command no transport udp under sip-ua configuration mode. This is because, phones register to the Unified SRST device using UDP for signaling transport with the non-secure SIP SRST configuration.

Playback of MOH from the flash memory of the router is supported for SIP lines in SRST mode in a co-located deployment of Unified SRST and Cisco Unified Border Element. Cisco IOS XE Fuji 16.7.1 and later releases support this feature.

Redundancy is not supported for the co-located deployment of Unified SRST and Unified Border Element.

Virtual interfaces are not supported for the co-located deployment of Unified SRST and Unified Border Element.

Configure Media Inactivity Timer to enable router to monitor and disconnect calls if no Real-Time Protocol (RTP) packets are received within a configurable time period. A sample configuration is as follows:

```
ip rtcp report interval 9000
gateway
  media-inactivity-criteria all
timer receive-rtp 1200
timer receive-rtcp 5
```
Restrictions

The following restrictions are observed for a co-located deployment of Unified SRST and Unified Border Element:

- You need to disable the NAT firewall support for SIP trunk side, using the CLI commands `no ip nat service sip udp port 5060` and `no ip nat service sip tcp port 5060`.
- All the SIP trunk features are not supported in a Unified SRST and Unified Border Element co-location deployment. For the list of supported features, see Unified SRST and Unified Border Element Co-location.

Examples

The following is a sample configuration for a voice class tenant:

```
voice class tenant 1
  registrar ipv4:10.64.86.64:5061:5061 scheme sips expires 240 tcp tls auth-realm
  sip-trunk.sample
  credentials number +492281844672 username xxxx password xxxx realm sip-trunk.sample
  authentication username xxxx password xxxx realm sip-trunk.sample
  no remote-party-id
  timers expires 900000
timers register 100
  sip-server dns:sip-trunk.sample:5061
  connection-reuse
  asserted-id pai
  bind control source-interface GigabitEthernet0/0/1
  bind media source-interface GigabitEthernet0/0/1
  conn-reuse
  sip-profiles 3000
  outbound-proxy dns:reg.sip-trunk.sample
  privacy-policy passthru
call-route p-called-party-id
  midcall-signaling preserve-codec
```

In the following configuration, the voice class tenant configured in the previous example is part of the dial-peer on the SIP trunk.

```
dial-peer voice 201 voip
description **SIP-TRUNK.SAMPLE**
  session protocol sipv2
  session target sip-server
  session transport tcp tls
destination e164-pattern-map 201
  incoming uri from 201
  voice-class codec 1
  voice-class sip url sips
  voice-class sip asserted-id pai
  voice-class sip outbound-proxy dns:reg.sip-trunk.sample
  voice-class sip tenant 1
  voice-class sip srtp-crypto 1
  voice-class sip bind control source-interface GigabitEthernet0/0/1
  voice-class sip bind media source-interface GigabitEthernet0/0/1
dtmf-relay rtp-nte
  srtp
  fax-relay ecm disable
  fax rate 14400
  ip qos dscp cs6 signaling
clid strip name
  no vad
```
Chapter 10      Configuring SIP Trunking on Unified SRST

The following example provides the **show running-config** command output for the co-located deployment of Unified SRST and Unified Border Element:

Building configuration...

Current configuration : 15564 bytes

<table>
<thead>
<tr>
<th>Command Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 16.7</td>
</tr>
<tr>
<td>Service times</td>
</tr>
<tr>
<td>Platform qfp</td>
</tr>
<tr>
<td>Card type</td>
</tr>
<tr>
<td>Address-family</td>
</tr>
<tr>
<td>Exit-address-family</td>
</tr>
<tr>
<td>No logging queue-limit</td>
</tr>
<tr>
<td>No logging console</td>
</tr>
<tr>
<td>Ip host gauss-lnx.cisco.com 10.64.86.64</td>
</tr>
<tr>
<td>Ip name-server 8.41.20.1</td>
</tr>
<tr>
<td>Ip dhcp excluded-address 8.39.23.13 8.39.23.50</td>
</tr>
<tr>
<td>Ip dhcp pool phones</td>
</tr>
<tr>
<td>Network 8.39.0.0 255.255.0.0</td>
</tr>
<tr>
<td>Default-router 8.39.23.13</td>
</tr>
<tr>
<td>Domain-name cisco.com</td>
</tr>
<tr>
<td>Dns-server 8.39.23.13</td>
</tr>
</tbody>
</table>

building configuration
Chapter 10 Configuring SIP Trunking on Unified SRST

Unified SRST and Unified Border Element Co-location

subscriber templating

multilink bundle-name authenticated

trunk group 1

xsvc

crypto pki trustpoint sipgw1

serial-number

ip-address 8.39.23.13

subject-name CN=sipgw1

revocation-check crl

rsakeypair cisco123

crypto pki certificate chain sipgw1

certificate ca 01

certificate 02

quit

certificate ca 01
Unified SRST and Unified Border Element Co-location

40C8C609 62C90203 010001A3 63006130 0F060355 1D130101 FF040530 030101FF
300E0603 551D0801 01FF0404 03020186 300E0603 551D0801 01FF0404 03020186
81F8D772 85C426B5 59F569D5 9F550059 C80C6950 8F65B50C 62F5B50C 5A010059
quit

! voice service voip
ip address trusted list
ipv4 8.55.0.0 255.255.0.0
ipv4 10.64.0.0 255.255.0.0
address-hiding
mode border-element license capacity 50
media statistics
media bulk-stats
media disable-detailed-stats
allow-connections sip to sip
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
supplementary-service media-renegotiate
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
sip
registrar server expires max 240 min 60

! voice class uri 101 sip
host ipv4:10.64.86.136

! voice class uri 201 sip
host dns: sip-trunk.sample

! voice class uri 301 sip
host ipv4:10.64.86.138

voice class codec 1
codec preference 1 g711alaw
codec preference 2 g722-64
codec preference 3 g711ulaw

! voice class sip-profiles 3000
rule 1 request REGISTER sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
rule 2 request REGISTER sip-header To modify "<sips:(.*)"> "<sip:\1"
rule 3 request REGISTER sip-header From modify "<sips:(.*)"> "<sip:\1"
rule 4 request REGISTER sip-header Contact modify "<.*:.*@(.*)>"
"<sip:\1;transport=tl;bcn>"
rule 6 request REGISTER sip-header Proxy-Require add "Proxy-Require: gin"
rule 7 request REGISTER sip-header Require add "Require: gin"

! voice class sip-profiles 201
rule 1 request ANY sip-header P-Asserted-Identity modify "<sips:(.*)>" "<sip:+492824293220@sip-trunk.sample>"
rule 2 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
rule 3 request ANY sip-header To modify "<sips:(.*)>" "<sip:\1"
rule 4 request ANY sip-header From modify "<sips:(.*)>" "<sip:\1"
rule 5 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tl>"
rule 6 response ANY sip-header To modify "<sips:(.*)>" "<sip:\1"
rule 7 response ANY sip-header From modify "<sips:(.*)>" "<sip:\1"
rule 8 response ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tl>"
rule 9 request ANY sip-header Min-SE remove
rule 10 request ANY sip-header Diversion remove
rule 11 request ANY sdp-header Connection-Info remove
rule 12 response ANY sdp-header Connection-Info remove
rule 13 request INVITE sip-header Allow-Header modify "INFO," ""

voice class sip-profiles 101
rule 1 request INVITE sip-header Supported modify "100rel," ""

voice class sip-profiles 102
rule 1 request INVITE sip-header Privacy add "Privacy:id"
rule 2 request INVITE sip-header P-Called-Party-ID add "P-Called-Party-ID: sip:2001@10.64.86.64"

voice class sip-copylist 201
sip-header FROM

voice class e164-pattern-map 101
e164 +492284229322T

voice class e164-pattern-map 201
e164 11[02]
e164 11[68]T
e164 11[025]
e164 +T
e164 0T
e164 2...

voice class e164-pattern-map 301
e164 3...

voice class dpg 201

voice class dpg 101
dial-peer 201

voice class dpg 301
dial-peer 301

voice class server-group 1
ipv4 10.64.86.136
description "**CUCM Server Group**"

voice class sip-options-keepalive 101
up-interval 30
retry 3
transport tcp
sip-profiles 3000

tenant 1
registrar dns: sip-trunk.sample:5061 scheme sips expires 240 tcp tls auth-realm
sip-trunk.sample
credentials number +492281844672 username xxxx password 7 060506324F41 realm
sip-trunk.sample
authentication username xxxx password 7 121A0C041104 realm sip-trunk.sample
no remote-party-id

no timers expires 60000
timers register 100
timers buffer-invite 1000
timers dns registrar-cache ttl
sip-server dns:sip-trunk.sample:5061
connection-reuse
asserted-id pai
bind control source-interface GigabitEthernet0/0/1
bind media source-interface GigabitEthernet0/0/1
no pass-thru content custom-sdp
conn-reuse
sip-profiles 3000
outbound-proxy dns:reg.sip-trunk.sample
privacy-policy passthru
call-route p-called-party-id
midcall-signaling preserve-codec
!
voice class tenant 2
registrar dns:sip-trunk.sample:5060 expires 240 tcp auth-realm sip-trunk.sample
credentials number +492281844673 username xxxx password 7 030752180500 realm
sip-trunk.sample
authentication username xxxx password 7 121A0C041104 realm sip-trunk.sample
no remote-party-id
timers expires 900000
timers register 100
timers buffer-invite 10000
timers dns registrar-cache ttl
sip-server dns:sip-trunk.sample:5060
connection-reuse
asserted-id pai
bind control source-interface GigabitEthernet0/0/1
bind media source-interface GigabitEthernet0/0/1
no pass-thru content custom-sdp
conn-reuse
sip-profiles 3000
outbound-proxy dns:reg.sip-trunk.sample
privacy-policy passthru
call-route p-called-party-id
midcall-signaling preserve-codec
!
voice class tenant 3
registrar dns:sipp.sample:6600 expires 240 auth-realm sip-trunk.sample
credentials number +492281844672 username xxxx password 7 121A0C041104 realm
sip-trunk.sample
authentication username xxxx password 7 05080F1C2243 realm sip-trunk.sample
no remote-party-id
timers expires 900000
timers register 500
timers buffer-invite 1000
timers dns registrar-cache ttl
sip-server dns:sipp.sample
connection-reuse
asserted-id pai
bind control source-interface GigabitEthernet0/0/1
bind media source-interface GigabitEthernet0/0/1
no pass-thru content custom-sdp
conn-reuse
sip-profiles 3000
outbound-proxy dns:sipp.sample:6600
privacy-policy passthru
call-route p-called-party-id
midcall-signaling preserve-codec
!
voice class tenant 4
timers expires 60000
 timers buffer-invite 10000
 connection-reuse
 asserted-id pai
bind control source-interface GigabitEthernet0/0/0
bind media source-interface GigabitEthernet0/0/0
no pass-thru content custom-sdp
privacy-policy passatr

call-route p-called-party-id
midcall-signaling preserve-codec

voice class srtp-crypto 1
crypto 1 AES_CM_128_HMAC_SHA1_32
crypto 2 AES_CM_128_HMAC_SHA1_80

voice register global
default mode
no allow-hash-in-dn
max-dn 40
max-pool 40

voice register pool 1
id network 8.55.0.0 mask 255.255.0.0
dtmf-relay rtp-nte
voice-class codec 1

voice hunt-group 1 parallel
list 1001,1002,1003
timeout 15
statistics collect
pilot 1234

voice hunt-group 2 sequential
list 1002,1003,1004
timeout 5
statistics collect
pilot 2345

voice-card 0/1
dsp services dspfarm
no watchdog

license udi pid ISR4321/K9 sn FDO201115PV
license boot level uck9
license boot level securityk9
no license smart enable
diagnostic bootup level minimal

username xxxx privilege 15 password 0 cisco
username xxxx password 0 cisco

redundancy
mode none


template 1

interface GigabitEthernet0/0/0
  ip address 8.39.23.13 255.255.0.0
  ip nat inside
  media-type rj45
  negotiation auto

interface GigabitEthernet0/0/1
  ip address 10.64.86.64 255.255.0.0
  ip nat outside
  negotiation auto

interface Service-Engine0/1/0

vrf forwarding Mgmt-intf
  no ip address
  negotiation auto

  no ip nat service sip tcp port 5060
  no ip nat service sip udp port 5060
  ip nat pool pool1 8.39.0.0 8.39.255.255 netmask 255.255.0.0
  ip nat inside source list 100 interface GigabitEthernet0/0/1 overload
  ip forward-protocol nd
  ip http server
  no ip http secure-server
  ip tftp source-interface GigabitEthernet0/0/0
  ip tftp blocksize 1520
  ip rtp report interval 9000
  ip route 0.0.0.0 0.0.0.0 8.39.0.1
  ip route 10.0.0.0 255.0.0.0 10.64.86.1

ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr

ip access-list extended nat-list
  access-list 100 permit ip 8.39.23.0 0.0.0.255 any

no ip ssh server

no ip tftp

no ip http

no ip rtp

no ip route

tftp-server flash:fbi88xx.BE-01-010.sbn
  tftp-server flash:kern88xx.12-0-1MN-113.sbn
tftp-server flash:rootfs88xx.12-0-1MN-113.sbn

tftp-server flash:sb288xx.BE-01-020.sbn

tftp-server flash:sip88xx.12-0-1MN-113.loads

tftp-server flash:vc488xx.12-0-1MN-113.sbn
!

ipv6 access-list preauth_v6
  permit udp any eq domain
  permit tcp any eq domain
  permit icmp any nd-ns
  permit icmp any nd-na
  permit icmp any router-solicitation
  permit icmp any router-advertisement
  permit icmp any redirect
  permit udp any eq 547 any eq 546
  permit udp any eq 546 any eq 547
  deny ipv6 any any
!
control-plane
!

voip trunk group 1
  xsvc
!
uc wsapi
  message-exchange max-failures 99
  response-timeout 2
  source-address 8.39.23.13
  probing interval keepalive 60
  probing max-failures 2
  provider xcc
!
provider xsvc
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!

dial-peer voice 201 voip
  description **SIP-TRUNK.SAMPLE**
  session protocol sipv2
  session target sip-server
  session transport tcp tls
  destination e164-pattern-map 201
  incoming uri from 201
  voice-class codec 1
  voice-class sip url sipv2
  voice-class sip profiles 201
  voice-class sip tenant 1
  voice-class sip srtp-crypto 1
  dtmrf-relay rtp-npe
  srtp
  fax-relay ecm disable
  fax rate 14400
clid strip name
no vad
!
dial-peer voice 301 voip
description "SIP-TRUNK.SAMPLE"
session protocol sipv2
session target sip-server
destination e164-pattern-map 301
incoming uri from 201
voice-class codec 1
voice-class sip url sip
voice-class sip profiles 201
voice-class sip tenant 2
dtmf-relay rtp-nte
srtp fallback
fax-relay ecm disable
fax rate 14400
clid strip name
no vad
!
dial-peer voice 401 voip
description "SIP-TRUNK.SAMPLE"
destination-pattern 4...
session protocol sipv2
session target sip-server
session transport udp
incoming uri from 301
voice-class codec 1
voice-class sip url sip
voice-class sip profiles 201
voice-class sip tenant 3
dtmf-relay rtp-nte
fax-relay ecm disable
fax rate 14400
clid strip name
no vad
!
dial-peer voice 101 voip
description "CUCM/PBX"
destination-pattern .T
session protocol sipv2
session transport tcp
session server-group 1
destination dpg 101
incoming uri via 101
voice-class codec 1
no voice-class sip outbound-proxy
voice-class sip srtp negotiate cisco
voice-class sip profiles 102 inbound
voice-class sip tenant 4
voice-class sip srtp-crypto 1
voice-class sip options-keepalive profile 101
dtmf-relay rtp-nte
srtp fallback
fax-relay ecm disable
fax rate 14400
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback pass-through g711alaw
no vad
!

presence
!
gateway
media-inactivity-criteria all
timer receive-rtcp 5
timer receive-rtp 180
!
sip-ua
transport tcp tls v1.2
crypto signaling default trustpoint sipgw1
!
alias exec cl clear logg
alias exec rtp show voip rtp connections
alias exec pool show voice register pool all brief
!
line con 0
exec-timeout 0 0
password cisco
width 0
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
password cisco
login local
length 0
transport input all
!
!
!
!
!
!
end
Feature Information for Configuring SIP Trunking on Unified SRST

Table 10-1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS 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.

Note

Table lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 10-1 Feature Information for Configuring SIP Trunking on Unified SRST

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified SRST and Unified Border Element Co-location</td>
<td>Cisco IOS XE Fuji 16.7.1</td>
<td>Added Support for co-location of Unified SRST and Unified Border Element on Cisco 4000 Series Integrated Services Router.</td>
</tr>
</tbody>
</table>
Integrating Voicemail with Cisco Unified SRST

This chapter describes how to make your existing voicemail system run on phones connected to a Cisco Unified SRST router during Cisco Unified Communications Manager fallback.

Cisco Unified SRST also supports incoming and outgoing Session Initiation Protocol (SIP) calls to and from Cisco Unified IP phones and router voice gateway voice ports. SIP may be used in situations where the Cisco Unified SRST Router is separate from the PSTN gateway and the SRST and PSTN gateways are linked together using SIP (instead of H.323).

For more information about SIP, see *Cisco IOS SIP Configuration Guide*.

Contents

- Information About Integrating Voicemail with Cisco Unified SRST, page 331
- How to Integrate Voicemail with Cisco Unified SCCP and SIP SRST, page 333
- Configuring Message Waiting Indication (SIP Phones in SRST Mode), page 345
- How to Configure DTMF Relay for SIP Applications and Voicemail, page 350
- Where to Go Next, page 354

Information About Integrating Voicemail with Cisco Unified SRST

Cisco Unified SRST can send and receive voicemail messages from Cisco Unity and other voicemail systems during Cisco Unified CM fallback. When the WAN is down, a voicemail system with BRI or PRI access to the Cisco Unified SRST system uses ISDN signaling (see Figure 11-1). Systems with Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) access connect to a PSTN and use in-band dual tone multifrequency (DTMF) signaling (see Figure 11-2).

From Unified SRST Release 12.0 onwards, Unified SRST supports voicemail on IPv6 protocols for SIP IP phones.
Both configurations allow phone message buttons to remain active and calls to busy or unanswered numbers to be forwarded to the dialed numbers’ mailboxes.

Calls that reach a busy signal, calls that are unanswered, and calls made by pressing the message button are forwarded to the voicemail system. To make this happen, you must configure access from the dial peers to the voicemail system and establish routing to the voicemail system for busy and unanswered calls and for message buttons.

If the voicemail system is accessed over FXO or FXS, you must configure instructions (DTMF patterns) for the voicemail system so that it can access the correct voicemail system mailbox. If your voicemail system is accessed over BRI or PRI, no instructions are necessary because the voicemail system can log in to the calling phone’s mailbox directly.
How to Integrate Voicemail with Cisco Unified SCCP and SIP SRST

This section contains the following tasks:

- Configuring Direct Access to Voicemail, page 333 (Required)
- Configuring Message Buttons, page 336 (Required)
- Redirecting to Cisco Unified Communications Manager Gateway, page 339 (Required for BRI or PRI)
- Configuring Call Forwarding to Voicemail, page 339 (Required FXO or FXS)
- Configuring Message Waiting Indication (Cisco Unified SRST Routers), page 343 (Optional)

**Note** Support for SIP SRST is added from IOS release 15.1(4)M3 and 15.2(1)T2.

Configuring Direct Access to Voicemail

You can configure direct access to voicemail system using BRI/PRI or FXO/FXS. To access voicemail messages with BRI/PRI or FXO/FXS access, you must have POTS dial peers configured with a destination pattern that matches the voicemail system’s number. Also, you must associate the dial peer with the port to which the voicemail system is accessed.

Both sets of configurations are done in dial-peer configuration mode. The summary and detailed steps below include only the basic commands necessary to perform this task. You may require additional commands for your particular dial-peer configuration.

**SUMMARY STEPS**

1. `dial-peer voice tag {pots | voatm | vofr | voip}
2. destination-pattern [+] string [T]
3. port {slot-number/subunit-number/port | slot/port:ds0-group-no}
4. forward-digits {num-digit | all | extra}
5. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;**dial-peer voice tag (pots</td>
<td>voatm</td>
</tr>
</tbody>
</table>
| **Example:**<br>Router(config)# **dial-peer voice 1002 pots** | *tag*: Digits that define a particular dial peer. Range is from 1 to 2147483647.  
*pots*: Indicates that this is a POTS dial peer that uses VoIP encapsulation on the IP backbone.  
*voatm*: Specifies that this is a VoATM dial peer that uses real-time AAL5 voice encapsulation on the ATM backbone network.  
*vofr*: Specifies that this is a VoFR dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network.  
*voip*: Indicates that this is a VoIP dial peer that uses voice encapsulation on the POTS network. |
| **Step 2**<br>**destination-pattern (+) string [T]** | (FXO or FXS and BRI or PRI) Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer. |
| **Example:**<br>Router(config-dial-peer)# **destination-pattern 1100T** | *+: (Optional) Character that indicates an E.164 standard number.  
*string*: See Table 11.1.  
*T*: (Optional) Control character that indicates that the destination-pattern value is a variable-length dial string. |
| **Step 3**<br>**port (slot-number/subunit-number/port | slot/port|ds0-group-no)** | (FXO or FXS and BRI or PRI) Associates a dial peer with a specific voice port on Cisco routers. |
| **Example:**<br>Router(config-dial-peer)# **port 1/1/1** | *slot-number*: Number of the slot in the router in which the voice interface card (VIC) is installed. Valid entries are from 0 to 3, depending on the slot in which it is installed.  
*subunit-number*: Subunit on the VIC in which the voice port is located. Valid entries are 0 or 1.  
*port*: Voice port number. Valid entries are 0 and 1.  
*ds0-group-no*: Specifies the DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card. |
### Step 4

**forward-digits (num-digit | all | extra)**

*(Optional for FXO or FXS)* Specifies which digits to forward for voice calls.

- **num-digit**: The number of digits to be forwarded. If the number of digits is greater than the length of a destination phone number, the length of the destination number is used. Range is 0 to 32. Setting the value to 0 is equivalent to entering the `no forward-digits` command.

- **all**: Forwards all digits. If `all` is entered, the full length of the destination pattern is used.

- **extra**: If the length of the dialed digit string is greater than the length of the dial-peer destination pattern, the extra right-justified digits are forwarded. However, if the dial-peer destination pattern is variable length and ends with the character “T” (for example: T, 123T, 123...T), extra digits are not forwarded.

**Example:**

```bash
Router(config-dial-peer)# forward-digits all
```

### Step 5

**exit**

*(FXO or FXS and BRI or PRI)* Exits dial-peer configuration mode.

**Example:**

```bash
Router(config-dial-peer)# exit
```

### Table 11-1 Valid Entries for the String Argument in the destination-pattern command

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digits 0 to 9</td>
<td>—</td>
</tr>
<tr>
<td>Letters A through D</td>
<td>—</td>
</tr>
<tr>
<td>Asterisk (*) and pound sign (#)</td>
<td>These appear on standard touch-tone dial pads.</td>
</tr>
<tr>
<td>Comma (,)</td>
<td>Inserts a pause between digits.</td>
</tr>
<tr>
<td>Period (.)</td>
<td>Matches any entered digit (this character is used as a wildcard).</td>
</tr>
<tr>
<td>Percent sign (%)</td>
<td>Indicates that the preceding digit occurred zero or more times; similar to the wildcard usage.</td>
</tr>
<tr>
<td>Plus sign (+)</td>
<td>Indicates that the preceding digit occurred one or more times.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The plus sign used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number.</td>
</tr>
<tr>
<td>Circumflex (^)</td>
<td>Indicates a match to the beginning of the string.</td>
</tr>
<tr>
<td>Parentheses ( ( ) ), which indicate a pattern and are the same as the regular expression rule.</td>
<td></td>
</tr>
<tr>
<td>Dollar sign ($)</td>
<td>Matches the null string at the end of the input string.</td>
</tr>
<tr>
<td>Backslash symbol ()</td>
<td>Is followed by a single character and matches that character. Can be used with a single character with no other significance (matching that character).</td>
</tr>
<tr>
<td>Question mark (?)</td>
<td>Indicates that the preceding digit occurred zero or one time.</td>
</tr>
<tr>
<td>Brackets ([ ])</td>
<td>Indicates a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range.</td>
</tr>
</tbody>
</table>
Examples

The following FXO and FXS example sets up a POTS dial peer named 1102, matches dial-peer 1102 to voicemail extension 1101, and assigns dial-peer 1102 to voice-port 1/1/1 where the voicemail system is connected. Other dial peers are configured for direct access to voicemail.

```conf
voice-port 1/1/1
timing digit 250
timing inter-digit 250
dial-peer voice 1102 pots
destination-pattern 1101
port 1/1/1
forward-digits all
dial-peer voice 1103 pots
destination-pattern 1101
port 1/1/1
forward-digits all
dial-peer voice 1104 pots
destination-pattern 1101
port 1/1/1
forward-digits all
```

The following example sets up a POTS dial peer named 1102 to go directly to 1101 through port 2/0:23:

```conf
controller T1 2/0
framing esf
clock source line primary
linecode b8zs
cablelength short 133
pri-group timeslots 21-24
interface Serial2/0:23
no ip address
no logging event link-status
isdn switch-type primary-net5
isdn incoming-voice voice
isdn T309-enable
no cdp enable
voice-port 2/0:23
dial-peer voice 1102 pots
destination-pattern 1101T
port 2/0:23
```

Configuring Message Buttons

To activate the message buttons on Cisco Unified IP phones connected to the Cisco Unified SCCP and SIP SRST router during Cisco Unified Communications Manager fallback, you must program a speed-dial number to the voicemail system. The speed-dial number is dialed when message buttons on phones connected to the Cisco Unified SCCP and SIP SRST router are pressed during Cisco Unified CM fallback. In addition, call forwarding must be configured so that calls to busy and unanswered numbers are sent to the voicemail number.

This configuration is required for FXO or FXS and BRI or PRI.
SUMMARY STEPS

1. call-manager-fallback
2. voicemail phone-number
3. call-forward busy directory-number
4. call-forward noan directory-number timeout seconds
5. exit
6. voice register pool tag
7. call-forward b2bua busy directory-number
8. call-forward b2bua noan directory-number timeout seconds
9. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td>Step 2 voicemail phone-number</td>
<td>Configures the telephone number that is dialed when the message button on a Cisco Unified SCCP IP Phone is pressed.</td>
</tr>
<tr>
<td>Example:</td>
<td>phone-number: Phone number configured as a speed-dial number for retrieving messages.</td>
</tr>
<tr>
<td>Router(config-cm-fallback)# voicemail 5550100</td>
<td></td>
</tr>
<tr>
<td>Step 3 call-forward busy directory-number</td>
<td>Configures call forwarding to another number when the Cisco SCCP IP phone is busy.</td>
</tr>
<tr>
<td>Example:</td>
<td>directory-number: Selected directory number representing a fully qualified E.164 number. This number can contain “.&quot; wildcard characters that correspond to the right-justified digits in the directory number extension.</td>
</tr>
<tr>
<td>Router(config-cm-fallback)# call-forward busy 2000</td>
<td></td>
</tr>
<tr>
<td>Step 4 call-forward noan directory-number timeout seconds</td>
<td>Configures call forwarding to another number when no answer is received from the Cisco SCCP IP phone.</td>
</tr>
<tr>
<td>Example:</td>
<td>directory-number: Selected directory number representing a fully qualified E.164 number. This number can contain “.” wildcard characters that correspond to the right-justified digits in the directory number extension.</td>
</tr>
<tr>
<td>Router(config-cm-fallback)# call-forward noan 2000 timeout 10</td>
<td>timeout seconds: Sets the waiting time, in seconds, before the call is forwarded to another phone. The seconds range is from 3 to 60000.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 5** | exit  
**Example:**  
Router(config-cm-fallback)# exit  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
**Step 6** | voice register pool tag  
**Example:**  
Router(config)# voice register pool 1  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
**Step 7** | call-forward b2bua busy directory-number  
**Example:**  
Router(config-register-pool)# call-forward b2bua busy 2000  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
**Step 8** | call-forward b2bua noan directory-number timeout seconds  
**Example:**  
Router(config-register-pool)# call-forward noan 2000 timeout 10  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
**Step 9** | exit  
**Example:**  
Router(config-register-pool)# exit  

### Examples

The following example specifies 1101 as the speed-dial number that is issued when message buttons are pressed on Cisco Unified IP Phones connected to the Cisco Unified SRST router. All busy and unanswered calls are configured to be forwarded to the voicemail number (1101).

```
call-manager-fallback  
voicemail 1101  
call-forward busy 1101  
call-forward noan 1101 timeout 3  
voice register pool 1  
call-forward b2bua busy 1101  
call-forward b2bua noan 1101 timeout 3
```
Redirecting to Cisco Unified Communications Manager Gateway

Note
The following task is required for voicemail systems with BRI or PRI access.

In addition to supporting message buttons for retrieving personal messages, Cisco Unified SRST allows the automatic forwarding of calls to busy and unanswered numbers to voicemail systems. Voicemail systems with BRI or PRI access can log in to the calling phone’s mailbox directly. For this to happen, some Cisco Unified CM configuration is recommended. If your voicemail system supports Redirected Dialed Number Identification Service (RDNIS), RDNIS must be included in the outgoing SETUP message to Cisco Unified CM to declare the last redirected number and the originally dialed number to and from configured devices and applications.

Step 1
From any page in Cisco Unified CM, click Device and Gateway.

Step 2
From the Find and List Gateways page, click Find.

Step 3
From the Find and List Gateways page, choose a device name.

Step 4
From the Gateway Configuration page, check Redirecting Number IE Delivery - Outgoing.

Configuring Call Forwarding to Voicemail

Note
The following task is required for voicemail systems with FXO or FXS access.

In addition to supporting message buttons for retrieving personal messages, Cisco Unified SRST allows the automatic forwarding of calls to busy or unanswered numbers to voicemail systems. The forwarded calls can be routed to almost any location in the voicemail system. Typically, calls are forwarded to a location in the called number’s mailbox where the caller can leave messages.

Call Routing Instructions Using DTMF Digit Patterns

Cisco Unified SRST call-routing instructions are required so that forwarded calls can be sent to the correct voicemail boxes. These instructions consist of DTMF digits configured in patterns that match the dial sequences required by the voicemail system to get to a particular voicemail location. For example, a voicemail system may be designed so that callers must do the following to leave a message:

1. Dial the central voicemail number (1101) and press #.
2. Dial an extension number (6000) and press #.
3. Dial 2 to select the menu option for leaving messages in the extension number’s mailbox.

For Cisco Unified SRST to forward a call to a busy or unanswered number to extension 6000’s mailbox, it must be programmed to issue a sequence of 1101#6000#2. As shown in Figure 11-3, this is accomplished through the voicemail and pattern commands.
How to Integrate Voicemail with Cisco Unified SCCP and SIP SRST

Figure 11-3  How Voicemail Dial Sequence 1101#6000#2 Is Configured in Cisco Unified SRST

The # cgn #2, # cdn #2, and # fdn #2 portions of the pattern commands shown in Figure 11-3 are DTMF digit patterns. These patterns are composed of tags and tokens. Tags are sets of characters representing DTMF tones. Tokens consist of three command keywords (cgn, cdn, and fdn) that declare the state of an incoming call transferred to voicemail.

A tag can be up to three character from the DTMF tone set (A to D, 0 to 9, # and *). Voicemail systems can use limited sets of DTMF tones. For example, Cisco Unity uses all DTMF tones but A to D. Tones can be defined in multiple ways. For example, when the star (*) is placed in front of a token by itself, it can mean “dial the following token number,” or, if it is at the end of a token, it can mark the end of a token number. If the asterisk is between other tag characters, it can mean dial *. The use of tags depends on how DTMF tones are defined by your voicemail system.

Tokens tell Cisco Unified SRST what telephone number in the call forwarding chain to use in the pattern. As shown in Figure 11-4, there are three types of tokens that correspond to three possible call states during voicemail forwarding.

Figure 11-4  How Numbers Are Extracted from Tokens

Sets of tags and tokens or patterns activate a voicemail system when one of the following occurs:

- A user presses the message button on a phone (pattern direct command).
- An internal extension attempts to connect to a busy extension and the call is forwarded to voicemail (pattern ext-to-ext busy command).
- An internal extension fails to connect to an extension and the call is forwarded to voicemail (pattern ext-to-ext no-answer command).
- An external trunk call reaches a busy extension and the call is forwarded to voicemail (pattern trunk-to-ext busy command).
An external trunk call reaches an unanswered extension and the call is forwarded to voicemail (pattern trunk-to-ext no-answer command).

Prerequisites

FXO hairpin-forwarded calls to voicemail systems must have disconnect supervision from the central office. For further information, see the FXO Answer and Disconnect Supervision document.

To configure patterns that your voicemail system will interpret correctly, you must know how the system routes voicemail calls and interprets DTMF tones (see the “Call Routing Instructions Using DTMF Digit Patterns” section on page 339).

You can find information about how Cisco Unity handles voicemail calls in the How to Transfer a Caller Directly into a Cisco Unity Mailbox document. Additional call-handling information can be found in the “Subscriber and Operator Orientation” chapters of any Cisco Unity system administration guide.

For other voicemail systems, see the analog voicemail integration configuration guide or information about the system’s call handling.

SUMMARY STEPS

1. vm-integration
2. pattern direct \(tag1\) {CGN | CDN | FDN} \(\tag2\) {CGN | CDN | FDN} \(\tag3\) {CGN | CDN | FDN} \(\last\)
3. pattern ext-to-ext busy \(tag1\) {CGN | CDN | FDN} \(\tag2\) {CGN | CDN | FDN} \(\tag3\) {CGN | CDN | FDN} \(\last\)
4. pattern ext-to-ext no-answer \(tag1\) {CGN | CDN | FDN} \(\tag2\) {CGN | CDN | FDN} \(\tag3\) {CGN | CDN | FDN} \(\last\)
5. pattern trunk-to-ext busy \(tag1\) {CGN | CDN | FDN} \(\tag2\) {CGN | CDN | FDN} \(\tag3\) {CGN | CDN | FDN} \(\last\)
6. pattern trunk-to-ext no-answer \(tag1\) {CGN | CDN | FDN} \(\tag2\) {CGN | CDN | FDN} \(\tag3\) {CGN | CDN | FDN} \(\last\)
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> vm-integration</td>
<td>Enters voicemail integration mode and enables voicemail integration with DTMF and analog voicemail systems.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config)# vm-integration
```

| **Step 2** pattern direct tag1 (CGN | CDN | FDN) [tag2 (CGN | CDN | FDN)] [tag3 (CGN | CDN | FDN)] [last-tag] | Configures the DTMF digit pattern forwarding necessary to activate the voicemail system when the user presses the messages button on the phone. |
|-----------------|----------------------------------|
| **Example:** | |
| Router(config-vm-int)# pattern direct 2 CGN * | |

**tag1:** Alphanumeric string fewer than four DTMF digits in length. The alphanumeric string consists of a combination of four letters (A, B, C, and D), two symbols (* and #), and ten digits (0 to 9). The tag numbers match the numbers defined in the voicemail system’s integration file, immediately preceding either the number of the calling party, the number of the called party, or a forwarding number.

**tag2** and **tag3:** (Optional) See **tag1**.

**last-tag:** See **tag1**. This tag indicates the end of the pattern.

**CGN:** Calling number (CGN) information is sent to the voicemail system.

**CDN:** Called number (CDN) information is sent to the voicemail system.

**FDN:** Forwarding number (FDN) information is sent to the voicemail system.

| **Step 3** pattern ext-to-ext busy tag1 (CGN | CDN | FDN) [tag2 (CGN | CDN | FDN)] [tag3 (CGN | CDN | FDN)] [last-tag] | Configures the DTMF digit pattern forwarding necessary to activate the voicemail system once an internal extension attempts to connect to a busy extension and the call is forwarded to voicemail. For argument and keyword information, see **Step 2**. |
|-----------------|----------------------------------|
| **Example:** | |
| Router(config-vm-int)# pattern ext-to-ext busy 7 FDN * CGN * | |

| **Step 4** pattern ext-to-ext no-answer tag1 (CGN | CDN | FDN) [tag2 (CGN | CDN | FDN)] [tag3 (CGN | CDN | FDN)] [last-tag] | Configures the DTMF digit pattern forwarding necessary to activate the voicemail system once an internal extension fails to connect to an extension and the call is forwarded to voicemail. For argument and keyword information, see **Step 2**. |
|-----------------|----------------------------------|
| **Example:** | |
| Router(config-vm-int)# pattern ext-to-ext no-answer 5 FDN * CGN * | |
### How to Integrate Voicemail with Cisco Unified SCCP and SIP SRST

#### Examples

For the following configuration, if the voicemail number is 1101, and 3001 is a phone with a message button, 1101*3001 would be dialed automatically when the 3001 message button is pressed. Under these circumstances, 3001 is considered to be a calling number or inbound call number.

```text
vm-integration
pattern direct * CGN *
```

For the following configuration, if 3001 calls 3006 and 3006 does not answer, the Unified SRST router will forward 3001 to the voicemail system (1101) and send to the voicemail system the DTMF pattern #3006 #2. This pattern is intended to select voicemail box number 3006 (3006’s voice mailbox). For this pattern to be sent, 3001 must be a forwarding number.

```text
vm-integration
pattern ext-to-ext no-answer # FDN #2
```

For the following configuration, if 3006 is busy and 3001 calls 3006, the Unified SRST router will forward 3001 to the voicemail system (1101) and send to the voicemail system the DTMF pattern #3006 #2. This pattern is intended to select voice mailbox number 3006 (3006’s voice mailbox). For this pattern to be sent, 3001 must be a forwarding number.

```text
vm-integration
pattern ext-to-ext busy # FDN #2
```

### Configuring Message Waiting Indication (Cisco Unified SRST Routers)

The Message Waiting Indication (MWI) relay mechanism is initiated after someone leaves a voicemail message on the remote voicemail message system. MWI relay is required when one Cisco Unity Voicemail system is shared by multiple Cisco Unified SRST routers. Unified SRST routers use the SIP Subscribe and Notify methods for MWI. See [Configuring Cisco IOS SIP Configuration Guide](#) for more information on SIP MWI and the Subscribe and Notify methods. The Unified SRST router that is the SIP MWI relay server acts as the SIP notifier. The other remote routers act as the SIP subscribers.
Restriction

- MWI is not supported during a fallback to Unified SRST. The MWI (the phone LED indication) will not correctly reflect when new messages arrive or when all messages have been listened to. We recommend resynchronizing MWIs after the WAN link is available, and connection with Unified Communications Manager is reestablished. The MWI behavior is consistent across voicemail support for IPv4 as well as IPv6 on Unified SRST.

### SUMMARY STEPS

1. call-manager-fallback
2. mwi relay
3. mwi reg-e164
4. exit
5. sip-ua
6. mwi-server {ipv4:destination-address | dns:host-name} [expires seconds] [port port] [transport {tcp | udp}] [unsolicited]
7. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> mwi relay</td>
<td>Enables the Unified SRST router to relay MWI information to remote Cisco IP phones.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# mwi relay</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mwi reg-e164</td>
<td>Registers E.164 numbers rather than extension numbers with a SIP proxy or registrar.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# mwi reg-e164</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# sip-ua</td>
<td></td>
</tr>
</tbody>
</table>
How to Integrate Voicemail with Cisco Unified SCCP and SIP SRST

Chapter 11  Integrating Voicemail with Cisco Unified SRST

Configuring Message Waiting Indication (SIP Phones in SRST Mode)

On SIP phones operating in the SIP SRST mode, you can use the `mwi unsolicited` command to configure a message-waiting notification when a message is sent by the Cisco Unity Express (CUE). The SIP phone then displays the notification when indicated by the voice messaging system. To configure message-waiting notification, perform the following steps.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `sip-ua`
4. `mwi-server [ipv4:destination-address | dns:host-name] [unsolicited]`
5. `exit`
6. `voice register global`

**Example:**

```
Router(config-sip-ua)# enable
Router(config-sip-ua)# configure terminal
Router(config-sip-ua)# sip-ua
Router(config-sip-ua)# mwi-server ipv4:10.0.2.254
Router(config-sip-ua)# exit
Router(config-sip-ua)# voice register global
```

---

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 6 `mwi-server [ipv4:destination-address | Configures voicemail server settings on a voice gateway or user agent. The IP address and port for the SIP-based MWI server should be in the same LAN as the voicemail server. The MWI server is a Cisco Unified SRST router. Keywords and arguments are as follows:
|  |_UNSOLICITED] | |
| `dns:host-name`) [expires seconds] [port port] [transport {tcp | udp}] [UNSOLICITED] | |
| Example: `Router(config-sip-ua)# mwi-server ipv4:10.0.2.254` | |

**Step 7**

- `exit`

**Example:**

```
Router(config-sip-ua)# exit
```

Exits SIP user-agent configuration mode.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>sip-ua</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# sip-ua</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**mwi-server (ipv4:destination-address</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config-sip-ua)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>voice register global</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# voice register global</td>
</tr>
</tbody>
</table>
This section provides the following configuration examples:

- Configuring Local Voicemail System (FXO and FXS): Example, page 347
- Configuring Central Location Voicemail System (FXO and FXS): Example, page 348
- Configuring Voicemail Access over FXO and FXS: Example, page 348
- Configuring Voicemail Access over BRI and PRI: Example, page 349
- Message Waiting Indication for SIP SRST: Example, page 350

### Configuring Local Voicemail System (FXO and FXS): Example

The “Dial-Peer Configuration for Integration of Voicemail with Cisco Unified SRST” section of the example below shows a legacy dial-peer configuration for a local voicemail system. The “Cisco Unified SRST Voicemail Integration Pattern Configuration” section must be compatible with your voicemail system configuration.

```plaintext
! Dial-Peer Configuration for Integration of voicemail with Cisco Unified SRST
!
dial-peer voice 101 pots
destination-pattern 14011
port 3/0/0
!
dial-peer voice 102 pots
preference 1
destination-pattern 14011
port 3/0/1
!
dial-peer voice 103 pots
preference 2
destination-pattern 14011
port 3/1/0
!
dial-peer voice 104 pots
destination-pattern 14011
port 3/1/1
!
! Cisco Unified SRST configuration
!
call-manager-fallback
 max-ephones 24
 max-dn 144
```

### Configuration Examples for Unified SRST

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>mwi unsolicited</code></td>
<td>Enables all SIP phones to receive MWI notification.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-register-global)# mwi unsolicited</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-register-global)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Unified SRST

Chapter 11      Integrating Voicemail with Cisco Unified SRST

Configuration Examples for Unified SRST

[Code Snippet]

voicemail 14011
call-forward busy 14011
call-forward noan 14011 timeout 3

! Cisco Unified SRST voicemail Integration Pattern Configuration

vm-integration
pattern direct 2 CGN *
pattern ext-to-ext no-answer 5 FDN * CGN *
pattern ext-to-ext busy 7 FDN * CGN *
pattern trunk-to-ext no-answer 4 FDN * CGN *
pattern trunk-to-ext busy 6 FDN * CGN *

Configuring Central Location Voicemail System (FXO and FXS): Example

The “Dial-Peer Configuration for Integration of voicemail with Cisco Unified SRST in Central Location” section of the example shows a legacy dial-peer configuration for a central voicemail system. The “Cisco Unified SRST Voicemail Integration Pattern Configuration” section must be compatible with your voicemail system configuration.

Note

Message waiting indicator (MWI) integration is not supported for PSTN access to voicemail systems at central locations.

[Code Snippet]

! Dial-Peer Configuration for Integration of voicemail with Cisco Unified SRST in Central Location
!
dial-peer voice 101 pots
destination-pattern 14011
port 3/0/0
!
! Cisco Unified SRST configuration
!
call-manager-fallback
max-ephones 24
max-dn 144
ip source-address 1.4.214.104 port 2000
voicemail 14011
call-forward busy 14011
call-forward noan 14011 timeout 3
!
! Cisco Unified SRST Voicemail Integration Pattern Configuration
!
vm-integration
pattern direct 2 CGN *
pattern ext-to-ext no-answer 5 FDN * CGN *
pattern ext-to-ext busy 7 FDN * CGN *
pattern trunk-to-ext no-answer 4 FDN * CGN *
pattern trunk-to-ext busy 6 FDN * CGN *

Configuring Voicemail Access over FXO and FXS: Example

The following example shows how to configure the Cisco Unified SRST router to forward unanswered calls to voicemail. In this example, the voicemail number is 1101, the voicemail system is connected to FXS voice port 1/1/1, and the voice mailbox numbers are 3001, 3002, and 3006.
Configuring Voicemail Access over BRI and PRI: Example

The following example shows how to configure the Cisco Unified SRST router to forward unanswered calls to voicemail. In this example, the voicemail number is 1101, the voicemail system is connected to a BRI or PRI voice port, and the voice mailbox numbers are 3001, 3002, and 3006.

controller T1 2/0
framing esf
clock source line primary
linecode b8zs
cablelength short 133
pri-group timeslots 21-24

interface Serial2/0:23
no ip address
no logging event link-status
isdn switch-type primary-net5
isdn incoming-voice voice
isdn T309-enable
no cdp enable

voice-port 2/0:23
dial-peer voice 1102 pots
destination-pattern 1101T
direct-inward-dial
port 2/0:23
call-manager-fallback
timeouts interdigit 5
ip source-address 1.6.0.199 port 2000
max-ephones 24
max-dn 24
transfer-pattern 3...
How to Configure DTMF Relay for SIP Applications and Voicemail

DTMF relay for SIP applications can be used in two voicemail situations:

- **DTMF Relay Using SIP RFC 2833**, page 350
- **DTMF Relay Using SIP Notify (Nonstandard)**, page 352

For SIP SRST forwarding call to voicemail configuration, see the """" section on page 183.

**Note**

Voicemail number associate with SIP phone message button in SRST is configured by Cisco Unified Communications Manager (CUCM), and not configurable by SIP SRST. The administrator needs to know the voicemail number set by CUCM to configure proper dial peer to voicemail system in SIP SRST.

**DTMF Relay Using SIP RFC 2833**

Cisco Unified Skinny Client Control Protocol (SCCP) Phones, such as those used with Cisco Unified SRST systems, provide only out-of-band DTMF digit indications. To enable SCCP phones to send digit information to remote SIP-based IVR and voicemail applications, Cisco Unified SRST 3.2 and later versions provide conversion from the out-of-band SCCP digit indication to the SIP standard for DTMF relay, which is RFC 2833. You select this method in the SIP VoIP dial peer using the `dtmf-relay rtp-nte` command.

The SIP DTMF relay method is needed in the following situations:
When SIP is used to connect a Cisco Unified SRST system to a remote SIP-based IVR or voicemail application, such as Cisco Unity.

- When SIP is used to connect a Cisco Unified SRST system to a remote SIP-PSTN voice gateway that goes through the PSTN to a voicemail or IVR application.

**Note**

The need to use out-of-band DTMF relay conversion is limited to SCCP phones. SIP phones natively support in-band DTMF relay as specified in RFC 2833.

To enable SIP DTMF relay using RFC 2833, the commands in this section must be used on both originating and terminating gateways.

**SUMMARY STEPS**

1. `dial-peer voice tag voip`
2. `dtmf-relay rtp-nte`
3. `exit`
4. `sip-ua`
5. `notify telephone-event max-duration time`
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>dial-peer voice tag voip</code></td>
<td>Enters dial-peer configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config)# dial-peer voice 2 voip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>dtmf-relay rtp-nte</code></td>
<td>Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config-dial-peer)# dtmf-relay rtp-nte</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>exit</code></td>
<td>Exits dial-peer configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config-dial-peer)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>sip-ua</code></td>
<td>Enables SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router(config)# sip-ua</code></td>
<td></td>
</tr>
</tbody>
</table>
How to Configure DTMF Relay for SIP Applications and Voicemail

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><code>dial-peer voice 123 voip</code></td>
<td>Configures the maximum time interval allowed between two consecutive NOTIFY messages for a single DTMF event.</td>
</tr>
<tr>
<td></td>
<td><code>dtmf-relay sip-notify</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>exit</code></td>
<td>Exits SIP user-agent configuration mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>exit</code></td>
<td></td>
</tr>
</tbody>
</table>

#### Example:

```bash
Router(config-sip-ua)# notify telephone-event max-duration 2000

Router(config-sip-ua)# exit
```

#### Troubleshooting Tips

The dial-peer section of the `show running-config` command output displays DTMF relay status when it is configured, as shown in this excerpt:

```bash
dial-peer voice 123 voip
   destination-pattern [12]...
   monitor probe icmp-ping
   session protocol sipv2
   session target ipv4:10.8.17.42
   dtmf-relay rtp-nte
```

#### DTMF Relay Using SIP Notify (Nonstandard)

To use voicemail on a SIP network that connects to a Cisco Unity Express system, use a nonstandard SIP Notify format. To configure the Notify format, use the `sip-notify` keyword with the `dtmf-relay` command. Using the `sip-notify` keyword may be required for backward compatibility with Cisco Unified SRST Versions 3.0 and 3.1.

### SUMMARY STEPS

1. `dial-peer voice tag voip`
2. `dtmf-relay sip-notify`
3. `exit`
4. `sip-ua`
5. `notify telephone-event max-duration time`
6. `exit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</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> <code>Router(config)# dial-peer voice 2 voip</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>dtmf-relay sip-notify</code></td>
<td>Forwards DTMF tones using SIP NOTIFY messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-dial-peer)# dtmf-relay sip-notify</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>exit</code></td>
<td>Exits dial-peer configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-dial-peer)# exit</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>sip-ua</code></td>
<td>Enables SIP user-agent configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config)# sip-ua</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>notify telephone-event max-duration time</code></td>
<td>Configures the maximum time interval allowed between two consecutive NOTIFY messages for a single DTMF event.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-sip-ua)# notify telephone-event max-duration 2000</code></td>
<td>- <code>max-duration time</code>: Time interval between consecutive NOTIFY messages for a single DTMF event, in milliseconds. Range is from 500 to 3000. Default is 2000.</td>
</tr>
<tr>
<td>6</td>
<td><code>exit</code></td>
<td>Exits SIP user-agent configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <code>Router(config-sip-ua)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

### Troubleshooting Tips

The `show sip-ua status` command output displays the time interval between consecutive NOTIFY messages for a telephone event. In the following example, the time interval is 2000 ms:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP User Agent bind status(signaling):DISABLED
SIP User Agent bind status(media):DISABLED
SIP 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
```
Redirect (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: IPv4
Transport types supported: RTP/AVP udptl

Where to Go Next

If you want to configure video parameters, see the “Setting Video Parameters” section on page 355.
For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
Setting Video Parameters

This chapter describes how to set video parameters for a Cisco Unified Survivable Remote Site Telephony (SRST) Router.

Contents

- Prerequisites for Setting Video Parameters, page 355
- Restrictions for Setting Video Parameters, page 356
- Information About Setting Video Parameters, page 356
- How to Set Video Parameters for Cisco Unified SRST, page 359
- Troubleshooting Video for Cisco Unified SRST, page 368
- Where to Go Next, page 368

Prerequisites for Setting Video Parameters

- Ensure that you are using Cisco Unified SRST 4.0 or a later version.
- Ensure that you are using Cisco Unified CM 4.0 or a later version.
- Ensure that the Cisco IP phones are registered with the Cisco Unified SRST router. Use the `show ephone registered` command to verify ephone registration.
- Ensure that the connection between the Cisco Unified Video Advantage application and the Cisco Unified IP phone is up.
  From a PC with Cisco Unified Video Advantage 1.02 or a later version installed, ensure that the line between the Cisco Unified Video Advantage and the Cisco Unified IP phone is green. For more information, see Cisco Unified Video Advantage End User Guides.
- Ensure that the correct video firmware is installed on the Cisco Unified IP phone. Use the `show ephone phone-load` command to view current ephone firmware. The following lists the minimum firmware version for video-enabled Cisco Unified IP phones:
  - Cisco Unified IP Phone 7940G version 6.0(4)
  - Cisco Unified IP Phone 7960G version 6.0(4)
  - Cisco Unified IP Phone 7970G version 6.0(2)
Restrictions for Setting Video Parameters

- This feature supports only the following video codecs:
  - H.261
  - H.263
  - H.264 (for CUVA from SRST 7.1)
- This feature supports only the following video formats:
  - Common Intermediate Format (CIF): Resolution 352x288
  - One-Quarter Common Intermediate Format (QCIF): Resolution 176x144
  - Sub QIF (SQCIF): Resolution 128x96
  - 4CIF: Resolution 704x576
  - 16CIF: Resolution 1408x1152
- The call start fast feature is not supported with an H.323 video connection. You must configure call start slow for H.323 video.
- Video capabilities are configured per ephone, not per line.
- All call feature controls (for example, mute and hold) apply to both audio and video calls, if applicable.
- This feature does not support the following:
  - Dynamic addition of video capability: The video capability must be present before the call setup starts to allow the video connection.
  - T-120 data connection between two SCCP endpoints
  - Video security
  - Far-end camera control (FECC) for SCCP endpoints
  - Video codec renegotiation: The negotiated video codec must match or the call falls back to audio-only. The negotiated codec for the existing call can be used for a new call.
  - Video codec transcoding
- When a video-capable endpoint connects to an audio-only endpoint, the call falls back to audio-only. During audio-only calls, video messages are skipped.

Information About Setting Video Parameters

This feature allows you to set video parameters for the Cisco Unified SRST to maintain close feature parity with Cisco Unified CM. When the Cisco Unified SRST is enabled, Cisco Unified IP phones do not have to be reconfigured for video capabilities because all ephones retain the same configuration used
with Cisco Unified CM. However, you must enter call-manager-fallback configuration mode to set video parameters for Cisco Unified SRST. The feature set for video is the same as that for Cisco Unified SRST audio calls.

To set video parameters, you should understand the following concepts:

- Matching Endpoint Capabilities, page 357
- Retrieving Video Codec Information, page 357
- Call Fallback to Audio-Only, page 357
- Call Setup for Video Endpoints, page 357
- Flow of the RTP Video Stream, page 358

### Matching Endpoint Capabilities

Endpoint capabilities are stored in the Cisco Unified SRST during phone registration. These capabilities are used to match with other endpoints during call setup. Endpoints can update at any time; however, the router recognizes endpoint-capability changes only during call setup. If a video feature is added to a phone, the information about it is updated in the router’s internal data structure, but that information does not take effect until the next call. If a video feature is removed, the router continues to see the video capability until the call is terminated but no video stream is exchanged between the two endpoints.

**Note**
The endpoint-capability match is executed every time a new call is set up or an existing call is resumed.

### Retrieving Video Codec Information

Voice gateways use dial-peer configurations to retrieve codec information for audio codecs. Video codec selection is done by the endpoints and is not controlled by the H.323 service-provider interface (SPI) through dial-peer or other configuration. The video-codec information is retrieved from the SCCP endpoint using a capabilities request during call setup.

### Call Fallback to Audio-Only

When a video-capable endpoint connects to an audio-only endpoint, the call falls back to an audio-only connection. Also, for certain features such as conferencing, where video support is not available, the call falls back to audio-only.

Cisco Unified SRST routers use a call-type flag to indicate whether the call is video-capable or audio-only. The call-type flag is set to video when the video capability is matched or set to audio-only when connecting to an audio-only TDM or an audio-only SIP endpoint.

**Note**
During an audio-only connection, all video-related media messages are skipped.

### Call Setup for Video Endpoints

The process for handling SCCP video endpoints is the same as that for handling SCCP audio endpoints. The video call must be part of the audio call. If the audio call setup fails, the video call fails.
During call setup for video, media setup handling determines if a video-media path is required or not. If so, the corresponding video-media-path setup actions are taken.

- For an SCCP endpoint, video-media-path setup includes sending messages to the endpoints to open a multimedia path and start the multimedia transmission.
- For an H.323 endpoint, video-media-path setup includes an exchange between the endpoints to open a logical channel for the video stream.

A call-type flag is set during call setup on the basis of the endpoint-capability match. After call setup, the call-type flag is used to determine whether an additional video-media path is required. Call signaling is managed by the Cisco Unified CME router, and the media stream is directly connected between the two video-enabled SCCP endpoints on the same router. Video-related commands and flow-control messages are forwarded to the other endpoint. Routers do not interpret these messages.

### Call Setup Between Two Local SCCP Endpoints

For interoperation between two local SCCP endpoints (that exist on the same router), video call setup uses all existing audio-call-setup handling, except during media setup. During media setup, a message is sent to establish the video-media path. If the endpoint responds, the video-media path is established and a start-multimedia-transmission function is called.

### Call Setup Between SCCP and H.323 Endpoints

Call setup between SCCP and H.323 endpoints is the same as it is between SCCP endpoints except that, if video capability is selected, the event is posted to the H.323 call leg to send out a video open logical channel (OLC) and the gateway generates an OLC for the video channel. Because the router needs to both terminate and originate the media stream, video must be enabled on the router before call setup begins.

### Call Setup Between Two SCCP Endpoints Across an H.323 Network

If call setup between SCCP endpoints occurs across an H.323 network, the setup is a combination of the processes listed in the previous two sections. The router controls the video media setup between the two endpoints, and the event is posted to the H.323 call leg so that the gateway can generate an OLC.

### Flow of the RTP Video Stream

For video streams between two local SCCP endpoints, the Real-Time Transport Protocol (RTP) stream is in flow-around mode. For video streams between SCCP and H.323 endpoints or two SCCP endpoints on different Cisco Unified CME routers, the RTP stream is in flow-through mode.

- Media flow-around mode enables RTP packets to stream directly between the endpoints of a VoIP call without the involvement of the gateway. By default, the gateway receives the incoming media, terminates the call, and then reoriginates it on the outbound call leg. In flow-around mode, only signaling data is passed to the gateway, improving scalability and performance.
- Media flow-through mode involves the same video-media path as for an audio call. Media packets flow through the gateway, thus hiding the networks from each other.
To display information about RTP named-event packets, such as caller-ID number, IP address, and port for both the local and remote endpoints, use the `show voip rtp connection` command as shown in the following sample output:

```
Router# show voip rtp connections
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP  RmtRTP  LocalIP         RemoteIP
 1  102     103        18714    18158  10.1.1.1        192.168.1.1
 2  105     104        17252    19088  10.1.1.1        192.168.1.1
Found 2 active RTP connections
```

How to Set Video Parameters for Cisco Unified SRST

When the Cisco Unified SRST is enabled, Cisco Unified IP phones do not have to be reconfigured for video capabilities because all ephones retain the same configuration used with Cisco Unified CM. However, you can set video parameters for Cisco Unified SRST.

Setting Video parameters for Cisco Unified SRST involves the following tasks:

- Configuring Slow Connect Procedures, page 359
- Verifying Cisco Unified SRST, page 360
- Setting Video Parameters for Cisco Unified SRST, page 366

Configuring Slow Connect Procedures

Video streams require slow-connect procedures for Cisco Unified SRST. H.323 endpoints require a slow connect because the endpoint-capability match occurs after the connect message.

**Note**

For more information about slow-connect procedures, see *Configuring Quality of Service for Voice*.

Use the following procedure to configure slow-connect procedures.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. h323
5. call start slow
### How to Set Video Parameters for Cisco Unified SRST

#### 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>Router&gt; enable</td>
<td></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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> h323</td>
<td>Enters H.323 voice-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# h323</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> call start slow</td>
<td>Forces an H.323 gateway to use slow-connect procedures for all VoIP calls.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-serv-h323)# call start slow</td>
<td></td>
</tr>
</tbody>
</table>

#### Verifying Cisco Unified SRST

Use the following procedure to verify that the Cisco Unified SRST feature is enabled and to verify Cisco Unified IP phone configuration settings.

#### Summary Steps

1. enable
2. show running config
3. show call-manager-fallback all
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 show running config | Displays the entire contents of the running configuration file. |
| **Example:**      | Router# show running config |
| Step 3 show call-manager-fallback all | Displays the detailed configuration of all Cisco Unified IP phones, directory numbers, voice ports, and dial peers in your network while in fallback mode. |
| **Example:**      | Router# show call-manager-fallback all |

**Note**

Use the *Settings* display on the Cisco Unified IP phones in your network to verify that the default router IP address on the phones matches the IP address of the Cisco Unified SRST router.

**Examples**

The following example shows output from the `show call-manager-fallback all` command:

```
Router# show call-manager-fallback all
CONFIG (Version=3.3)  
=====================  
Version 3.3  
For on-line documentation please see:  

ip source-address 10.1.1.1 port 2000  
max-video-bit-rate 384(kbps)  
max-ephones 52  
max-dn 110  
max-conferences 16 gain -6  
dspfarm units 0  
dspfarm transcode sessions 0  
huntstop  
dialplan-pattern 1 4084442... extension-length 4  
voicemail 6001  
moh music-on-hold.au  
time-format 24  
date-format dd-mm-yy  
timezone 0 Greenwich Standard Time  
call-forward busy 6001  
call-forward noan 6001 timeout 8  
call-forward pattern .T  
transfer-pattern .T  
keepalive 45  
timeout interdigit 10  
timeout busy 10  
timeout ringing 180  
caller-id name-only: enable  
Limit number of DNs per phone:
Chapter 12  Setting Video Parameters

How to Set Video Parameters for Cisco Unified SRST

7910: 34
7935: 34
7936: 34
7940: 34
7960: 34
7970: 34

Log (table parameters):
  max-size: 150
    retain-timer: 15
transfer-system full-consult
local directory service: enabled.

ephone-dn 1
  number 1001
  name 1001
description 1001
label 1001
preference 0 secondary 9
huntstop
call-forward busy 6001
call-forward noan 6001 timeout 8
call-waiting beep

ephone-dn 2
  number 1002
  name 1002
description 1002
preference 0 secondary 9
huntstop
call-forward busy 6001
call-forward noan 6001 timeout 8
call-waiting beep

ephone-dn 3
  preference 0 secondary 9
  huntstop
call-waiting beep

ephone-dn 4
  preference 0 secondary 9
  huntstop
call-waiting beep

ephone-dn 5
  preference 0 secondary 9
  huntstop
call-waiting beep

ephone-dn 6
  preference 0 secondary 9
  huntstop
call-waiting beep

ephone-dn 7
  preference 0 secondary 9
  huntstop
call-waiting beep

ephone-dn 8
  preference 0 secondary 9
  huntstop
call-waiting beep

ephone-dn 9
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 10
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 11
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 12
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 13
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 14
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 15
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 16
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 17
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 18
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 19
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 20
preference 0 secondary 9
huntstop
call-waiting beep

Number of Configured ephones 0 (Registered 2)

voice-port 50/0/1
station-id number 1001
station-id name 1001
How to Set Video Parameters for Cisco Unified SRST

```bash
timeout ringing 8
voice-port 50/0/2
  station-id number 1002
  station-id name 1002
  timeout ringing 8
voice-port 50/0/3
voice-port 50/0/4
voice-port 50/0/5
voice-port 50/0/6
voice-port 50/0/7
voice-port 50/0/8
voice-port 50/0/9
voice-port 50/0/10
voice-port 50/0/11
voice-port 50/0/12
voice-port 50/0/13
voice-port 50/0/14
voice-port 50/0/15
voice-port 50/0/16
voice-port 50/0/17
voice-port 50/0/18
voice-port 50/0/19
voice-port 50/0/20

dial-peer voice 20055 pots
destination-pattern 1001
  huntstop
call-forward busy 6001
call-forward noan 6001
  progress_ind setup enable 3
  port 50/0/1

dial-peer voice 20056 pots
destination-pattern 1002
  huntstop
call-forward busy 6001
call-forward noan 6001
  progress_ind setup enable 3
  port 50/0/2

dial-peer voice 20057 pots
  huntstop
  progress_ind setup enable 3
  port 50/0/3
```
dial-peer voice 20058 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/4

dial-peer voice 20059 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/5

dial-peer voice 20060 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/6

dial-peer voice 20061 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/7

dial-peer voice 20062 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/8

dial-peer voice 20063 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/9

dial-peer voice 20064 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/10

dial-peer voice 20065 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/11

dial-peer voice 20066 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/12

dial-peer voice 20067 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/13

dial-peer voice 20068 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/14

dial-peer voice 20069 pots
    huntstop
    progress_ind setup enable 3
    port 50/0/15

dial-peer voice 20070 pots
    huntstop
    progress_ind setup enable 3
Setting Video Parameters for Cisco Unified SRST

Using the following procedure to set the maximum bit rate for all video-capable phones in a Cisco Unified SRST system.

```plaintext
port 50/0/16
dial-peer voice 20071 pots
huntstop
progress_ind setup enable 3
port 50/0/17
dial-peer voice 20072 pots
huntstop
progress_ind setup enable 3
port 50/0/18
dial-peer voice 20073 pots
huntstop
progress_ind setup enable 3
port 50/0/19
dial-peer voice 20074 pots
huntstop
progress_ind setup enable 3
port 50/0/20
tftp-server system:/its/SEPDEFAULT.cnf
tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
tftp-server system:/its/united_states/7960-tones.xml alias United_States/7960-tones.xml
tftp-server system:/its/united_states/7960-font.xml alias English_United_States/7960-font.xml
tftp-server system:/its/united_states/7960-dictionary.xml alias English_United_States/7960-dictionary.xml
tftp-server system:/its/united_states/7960-kate.xml alias English_United_States/7960-kate.xml
tftp-server system:/its/united_states/SCCP-dictionary.xml alias English_United_States/SCCP-dictionary.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000000.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000020.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000030.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000040.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000050.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000060.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000070.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000080.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000090.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD000000A0.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD000000B0.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD000000C0.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD000000D0.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000100.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000110.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000120.cnf.xml
```
SUMMARY STEPS

1. enable
2. configure terminal
3. call-manager-fallback
4. video
5. maximum bit-rate value

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>Router&gt; enable</td>
<td>Example:</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>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td>Step 4 video</td>
<td>Enters call-manager-fallback video configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-call-manager-fallback)#</td>
<td></td>
</tr>
<tr>
<td>video</td>
<td></td>
</tr>
<tr>
<td>Step 5 maximum bit-rate value</td>
<td>Sets the maximum IP phone video bandwidth, in kbps. The range is 0 to 10000000. The default is 10000000.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-cm-fallback-video)# maximum</td>
<td></td>
</tr>
<tr>
<td>bit-rate value</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following example shows the configuration for video with Cisco Unified SRST:

```
call-manager-fallback
  video
    maximum bit-rate 384
max-conferences 2 gain -6
transfer-system full-consult
ip source-address 10.0.1.1 port 2000
max-ephones 52
max-dn 110
dialplan-pattern 1 4084442... extension-length 4
transfer-pattern .T
keepalive 45
voicemail 6001
call-forward pattern .T
```
call-forward busy 6001
call-forward noan 6001 timeout 3
moh music-on-hold.au
time-format 24
date-format dd-mm-yy
!

Troubleshooting Video for Cisco Unified SRST

Use the following commands to troubleshoot Video for Cisco Unified SRST.

- For SCCP endpoint troubleshooting, use the following `debug` commands:
  - `debug ch323 video`: Enables video debugging trace on the H.323 SPI.
  - `debug ephone detail`: Debugs all Cisco Unified IP phones that are registered to the router and displays error and state levels.
  - `debug h225 asn1`: Displays Abstract Syntax Notation One (ASN.1) contents of H.225 messages that have been sent or received.
  - `debug h245 asn1`: Displays ASN.1 contents of H.245 messages that have been sent or received.
  - `debug voip ccapi inout`: Displays the execution path through the call-control-application programming interface (CPI).

- For ephone troubleshooting, use the following `debug` commands:
  - `debug ephone message`: Enables message tracing between Cisco ephones.
  - `debug ephone register`: Sets registration debugging for ephones.
  - `debug ephone video`: Sets ephone video traces, which provide information about different video states for the call, including video capabilities selection, start, and stop.

- For basic video-to-video call checking, use the following `show` commands:
  - `show call active video`: Displays call information for SCCP video calls in progress.
  - `show ephone offhook`: Displays information and packet counts for ephones that are currently off hook.
  - `show voip rtp connections`: Displays information about RTP named-event packets, such as caller ID number, IP address, and port, for both the local and remote endpoints.

Where to Go Next

To monitor and maintain Cisco Unified SRST, see the “Monitoring and Maintaining Cisco Unified SRST” section on page 369.

For additional information, see the “Additional References” section on page 29 in the “Cisco Unified SRST Feature Overview” section on page 1 chapter.
To monitor and maintain Cisco Unified Survivable Remote Site Telephony (SRST), use the following commands in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show call-manager-fallback all</td>
<td>Displays the detailed configuration of all the Cisco Unified IP phones, voice ports, and dial peers of the Cisco Unified SRST Router.</td>
</tr>
<tr>
<td>Router# show call-manager-fallback dial-peer</td>
<td>Displays the output of the dial peers of the Cisco Unified SRST Router.</td>
</tr>
<tr>
<td>Router# show call-manager-fallback ephone-dn</td>
<td>Displays Cisco Unified IP Phone destination numbers when in call manager fallback mode.</td>
</tr>
<tr>
<td>Router# show call-manager-fallback voice-port</td>
<td>Displays output for the voice ports.</td>
</tr>
<tr>
<td>Router# show dial-peer voice summary</td>
<td>Displays a summary of all voice dial peers.</td>
</tr>
<tr>
<td>Router# show ephone phone</td>
<td>Displays Cisco Unified IP Phone status.</td>
</tr>
<tr>
<td>Router# show ephone offhook</td>
<td>Displays Cisco Unified IP Phone status for all phones that are off hook.</td>
</tr>
<tr>
<td>Router# show ephone registered</td>
<td>Displays Cisco Unified IP Phone status for all phones that are currently registered.</td>
</tr>
<tr>
<td>Router# show ephone remote</td>
<td>Displays Cisco Unified IP Phone status for all nonlocal phones (phones that have no Address Resolution Protocol [ARP] entry).</td>
</tr>
<tr>
<td>Router# show ephone ringing</td>
<td>Displays Cisco Unified IP Phone status for all phones that are ringing.</td>
</tr>
<tr>
<td>Router# show ephone summary</td>
<td>Displays a summary of all Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Router# show ephone telephone-number phone-number</td>
<td>Displays Unified IP Phone status for a specific phone number.</td>
</tr>
<tr>
<td>Router# show ephone unregistered</td>
<td>Displays Unified IP Phone status for all unregistered phones.</td>
</tr>
<tr>
<td>Router# show ephone-dn tag</td>
<td>Displays Unified IP Phone destination numbers.</td>
</tr>
<tr>
<td>Router# show ephone-dn summary</td>
<td>Displays a summary of all Cisco Unified IP Phone destination numbers.</td>
</tr>
<tr>
<td>Router# show ephone-dn loopback</td>
<td>Displays Cisco Unified IP Phone destination numbers in loopback mode.</td>
</tr>
<tr>
<td>Router# show running-config</td>
<td>Displays the configuration.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Router # <code>show sip-ua status registrar</code></td>
<td>Display SIP registrar clients.</td>
</tr>
<tr>
<td>Router# <code>show voice port summary</code></td>
<td>Displays a summary of all voice ports.</td>
</tr>
<tr>
<td>Router # <code>show voice register all</code></td>
<td>Displays all SIP SRST configurations, SIP phone registrations and dial peer info.</td>
</tr>
<tr>
<td>Router # <code>show voice register global</code></td>
<td>Displays voice register global config.</td>
</tr>
<tr>
<td>Router # <code>show voice register pool all</code></td>
<td>Displays all config SIP phone voice register pool detail info.</td>
</tr>
<tr>
<td>Router # <code>show voice register pool &lt;tag&gt;</code></td>
<td>Displays specific SIP phone voice register pool detail info.</td>
</tr>
<tr>
<td>Router # <code>show voice register dial-peers</code></td>
<td>Displays SIP-SRST created dial peer.</td>
</tr>
<tr>
<td>Router # <code>show voice register dn all</code></td>
<td>Displays all config voice register dn detail info.</td>
</tr>
<tr>
<td>Router # <code>show voice register dn &lt;tag&gt;</code></td>
<td>Displays specific voice register dn detail info.</td>
</tr>
</tbody>
</table>
Configuring Cisco Unified SIP SRST Features Using Redirect Mode

Note
This chapter applies to version 3.0 only.

This chapter describes Cisco Unified Session Initiation Protocol (SIP) Survivable Remote Site Telephony (SRST) features using redirect mode.

Contents

- Prerequisites for Cisco Unified SIP SRST Features Using Redirect Mode, page A-1
- Restrictions for Cisco Unified SIP SRST Features Using Redirect Mode, page A-1
- Information About Cisco Unified SIP SRST Features Using Redirect Mode, page A-2
- How to Configure Cisco Unified SIP SRST Features Using Redirect Mode, page A-2
- Configuration Examples for Cisco Unified SIP SRST Features Using Redirect Mode, page A-6
- Where to Go Next, page A-8

Prerequisites for Cisco Unified SIP SRST Features Using Redirect Mode

Complete the prerequisites documented in the “Prerequisites for Configuring Cisco Unified SIP SRST” section on page 1-9 in the “Cisco Unified SRST Feature Overview” section on page 1-1.

Restrictions for Cisco Unified SIP SRST Features Using Redirect Mode

See the restrictions documented in the “Restrictions for Configuring Cisco Unified SIP SRST” section on page 1-10 section in the “Cisco Unified SRST Feature Overview” section on page 1-1.
Information About Cisco Unified SIP SRST Features Using Redirect Mode

Cisco Unified SIP SRST provides backup to an external SIP call control (IP-PBX) by providing basic registrar and redirect services. These services are used by a SIP IP phone in the event of a WAN connection outage when the SIP phone is unable to communicate with its primary SIP proxy. The Cisco Unified SIP SRST device also provides PSTN gateway access for placing and receiving PSTN calls.

To make maximum use of the Cisco Unified SIP SRST service, the local SIP IP phones should support dual (concurrent) registration with both their primary SIP proxy or registrar and the Cisco Unified SIP SRST backup registrar. Cisco Unified SIP SRST works for the following types of calls:

- Local SIP IP phone to local SIP phone, if the main proxy is unavailable.
- Additional services like class of restriction (COR) for local SIP IP phones to the outgoing PSTN. For example, to block outgoing 1-900 numbers.

How to Configure Cisco Unified SIP SRST Features Using Redirect Mode

This section contains the following procedures:

- Configuring Call Redirect Enhancements to Support Calls Between SIP IP Phones for Cisco Unified SIP SRST, page A-2 (required)
- Configuring Sending 300 Multiple Choice Support, page A-5 (required)

Configuring Call Redirect Enhancements to Support Calls Between SIP IP Phones for Cisco Unified SIP SRST

The call redirect enhancement supports calls from a local SIP phone to another local SIP phone through the Cisco IOS voice gateway. Prior to this enhancement, an attempt by a SIP phone to contact another local SIP phone using the Cisco IOS voice gateway as if it were a SIP proxy or redirect server would fail. However, the Cisco IOS voice gateway can now act as a SIP redirect server. The voice gateway responds to the originator with a SIP Redirect message, allowing the SIP phone that originated the call to establish a call to its destination.

The `redirect ip2ip` (voice service) and `redirect ip2ip` (dial-peer) commands allow you to enable the SIP functionality, globally or on a specific inbound dial peer. The default application on Cisco Unified SIP SRST supports IP-to-IP redirection.

- Configuring Call Redirect Enhancements to Support Calls Globally, page A-3
- Configuring Call Redirect Enhancements to Support Calls on a Specific VoIP Dial Peer, page A-4
Configuring Call Redirect Enhancements to Support Calls Globally

To enable global IP-to-IP call redirection for all VoIP dial peers, use voice service configuration mode.

**Note**
When IP-to-IP redirection is configured in dial-peer configuration mode, the configuration for the specific dial peer takes precedence over the global configuration entered under voice service configuration mode.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `redirect ip2ip`
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>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>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# voice service voip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> redirect ip2ip</td>
<td>Redirects SIP phone calls to SIP phone calls globally on a gateway using the Cisco IOS voice gateway.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-voi-srv)# redirect ip2ip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-voi-srv)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Call Redirect Enhancements to Support Calls on a Specific VoIP Dial Peer

To enable IP-to-IP call redirection for a specific VoIP dial peer, configure it on an inbound dial peer in dial-peer configuration mode. The default application on Cisco Unified SIP SRST supports IP-to-IP redirection.

Note
When IP-to-IP redirection is configured in dial-peer configuration mode, the configuration for the specific dial peer takes precedence over the global configuration entered under voice service configuration mode.

Restrictions
The redirect ip2ip command must be configured on an inbound dial peer of the gateway.

SUMMARY STEPS
1. enable
2. configure terminal
3. dial-peer voice tag voip
4. application application-name
5. redirect ip2ip
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></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</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>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial-peer configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>tag—A number that uniquely identifies the dial peer (this number has local significance only).</td>
</tr>
<tr>
<td></td>
<td>voip—Indicates that this is a VoIP peer using voice encapsulation on the POTS network and is used for configuring redirect.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# dial-peer voice 25 voip</td>
</tr>
</tbody>
</table>
How to Configure Cisco Unified SIP SRST Features Using Redirect Mode

Prior to Cisco IOS Release 12.2(15)ZJ, when a call was redirected, the SIP gateway would send a 302 Moved Temporarily message. The first longest match route on a gateway (dial-peer destination pattern) was used in the Contact header of the 302 message. With Release 12.2(15)ZJ, if multiple routes to a destination exist for a redirected number (multiple dial peers are matched), the SIP gateway sends a 300 Multiple Choice message, and the multiple routes in the Contact header are listed.

The configuration below allows users to choose the order in which the routes appear in the Contact header.

### Configuring Sending 300 Multiple Choice Support

Prior to Cisco IOS Release 12.2(15)ZJ, when a call was redirected, the SIP gateway would send a 302 Moved Temporarily message. The first longest match route on a gateway (dial-peer destination pattern) was used in the Contact header of the 302 message. With Release 12.2(15)ZJ, if multiple routes to a destination exist for a redirected number (multiple dial peers are matched), the SIP gateway sends a 300 Multiple Choice message, and the multiple routes in the Contact header are listed.

The configuration below allows users to choose the order in which the routes appear in the Contact header.

### SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. redirect contact order [best-match | longest-match]
6. end

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>application application-name</td>
<td>Enables a specific application on a dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# application session</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Redirects SIP phone calls to SIP phone calls on a specific VoIP dial peer using the Cisco IOS voice gateway.</td>
</tr>
<tr>
<td>redirect ip2ip</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# redirect ip2ip</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>
### 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.  
  
  * Enter your password if prompted. |
| 2    | configure terminal| Enters global configuration mode. |
| 3    | voice service voip| Enters voice service configuration mode. |
| 4    | sip               | Enters SIP configuration mode. |
| 5    | redirect contact order [best-match | longest-match] | Sets the order of contacts in the 300 Multiple Choice message. The keywords are defined as follows:  
  
  * **best-match**—(Optional) Uses the current system configuration to set the order of contacts.  
  
  * **longest-match**—(Optional) Sets the contact order by using the destination pattern longest match first, and then the second longest match, the third longest match, and so on. This is the default. |
| 6    | end               | Returns to privileged EXEC mode. |

### Configuration Examples for Cisco Unified SIP SRST Features Using Redirect Mode

This section provides the following configuration example:

- **Cisco Unified SIP SRST: Example, page A-7**
Cisco Unified SIP SRST: Example

This section provides a configuration example to match the configuration tasks in the previous sections.

```
! Sets up the registrar server and enables IP-to-IP redirection and 300
! Multiple Choice support.
! voice service voip
  redirect ip2ip
  sip
    registrar server expires max 600 min 60
    redirect contact order best-match
!
! Configures the voice-class codec with G.711uLaw and G729 codecs. The codecs are
! applied to the voice register pools.
! voice class codec 1
  codec preference 1 g711ulaw
  codec preference 2 g729br8
!
! The voice register pools define various pools that are used to match
! incoming REGISTER requests and create corresponding dial peers.
! voice register pool 1
  id mac 0030.94C2.A22A
  preference 5
  cor incoming call91 1 91011
  translate-outgoing called 1
  proxy 10.2.161.187 preference 1 monitor probe icmp-ping
  alias 94... to 91011 preference 8
  voice-class codec 1
!
voice register pool 2
  id ip 192.168.0.3 mask 255.255.255.255
  preference 5
  cor outgoing call95 1 91021
  proxy 10.2.161.187 preference 1
  voice-class codec 1
!
voice register pool 3
  id network 10.2.161.0 mask 255.255.255.0
  number 1 95... preference 1
  preference 5
  cor incoming call95 1 95011
  cor outgoing call95 1 95011
  proxy 10.2.161.187 preference 1 monitor probe icmp-ping
  max registrations 5
  voice-class codec 1
!
voice register pool 4
  id network 10.2.161.0 mask 255.255.255.0
  number 1 94... preference 1
  preference 5
  cor incoming everywhere default
  cor outgoing everywhere default
  proxy 10.2.161.187 preference 1
  max registrations 2
  voice-class codec 1
!
! Configures translation rules to be applied in the voice register pools.
! translation-rule 1
```
Where to Go Next

For additional information, see the “Additional References” section on page 1-29 in the “Cisco Unified SRST Feature Overview” section on page 1-1 chapter.
Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource

This chapter describes how to configure Cisco Unified CM and Cisco Unified SRST to allow Cisco Unified CM to use Cisco Unified SRST gateways as multicast music-on-hold (MOH) resources during fallback and normal Cisco Unified CM operation. A distributed MOH design with local gateways providing MOH eliminates the need to stream MOH across a WAN and saves bandwidth.

Finding Feature Information in This Module
Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the “Feature Information for Cisco Unified SRST as a Multicast MOH Resource” section on page B-42.

Contents

- Prerequisites for Using Cisco Unified SRST Gateways as a Multicast MOH Resource, page B-12
- Restrictions for Using Cisco Unified SRST Gateways as a Multicast MOH Resource, page B-12
- Information About Using Cisco Unified SRST Gateways as a Multicast MOH Resource, page B-13
- How to Use Cisco Unified SRST Gateways as a Multicast MOH Resource, page B-18
- Configurations Examples for Cisco Unified SRST Gateways, page B-41
- Where to Go Next, page B-43
Prerequisites for Using Cisco Unified SRST Gateways as a Multicast MOH Resource

- Multicast MOH for H.323 and MGCP is supported on Cisco Unified CM 3.1.1 and higher versions.
- Cisco Unified CM must be configured as follows:
  - With multicast MOH enabled.
  - With Media Resource Groups (MRGs) and Media Resource Group Lists (MRGLs) controlling which devices receive multicast MOH and which devices receive unicast MOH.
  - With Cisco Unified CM regions assigned so that G.711 is used whenever a Cisco Unified SRST multicast MOH resource is invoked.
- The Cisco Unified SRST gateways must run on Cisco Unified SRST 3.0 on Cisco IOS Release 12.2(15)ZJ2 or a later release.
- Cisco Unified SRST must be registered to Cisco Unified CM using protocol such as H.323, MGCP, or SIP.
- For branches that do not run Cisco Unified SRST, Cisco Unified CM multicast MOH packets must cross the WAN. To accomplish this, you must have multicast routing enabled in your network. For more information about multicast routing, see the “IP Multicast” section of Cisco IOS IP Configuration Guide, Release 12.4T.
- With Cisco IOS earlier than 12.3(14)T, configure Cisco Unified SRST as your MGCP gateway’s fallback mode using the `ccm-manager fallback-mgcp` and `call application alternate` commands. With Cisco IOS releases after 12.3(14)T, the `ccm-manager fallback-mgcp` and `service` commands must be configured. Configuring these two commands allows Cisco Unified SRST to assume control over the voice port and over call processing on the MGCP gateway. A complete configuration describing setting up Cisco Unified SRST as your fallback mode is shown in Cisco Unified Communications Manager Administration Guide, Release 5.1(3) Survivable Remote Site Telephony Configuration.

Restrictions for Using Cisco Unified SRST Gateways as a Multicast MOH Resource

- Cisco Unified SRST multicast MOH does not support unicast MOH.
- Only a single Cisco Unified CM audio source can be used throughout the network. However, the audio files on each Cisco Unified SRST gateway’s flash memory can be different.
- Cisco Unified SRST multicast MOH supports G.711 only.
- Unified SRST multicast MOH does not support co-location of tunnels on the same device.
- Multicast MOH support for H.323 is unavailable in all versions of Cisco Unified Communications Manager 3.3.2. For more information, see CSCdz00697 using the Bug Toolkit.
- In the Cisco IOS Release 12.2(15)ZJ image for Cisco 1700 series gateways, Cisco Unified SRST multicast MOH does not include support for H.323 mode.
Information About Using Cisco Unified SRST Gateways as a Multicast MOH Resource

To configure Cisco Unified SRST gateways as an MOH resource, you should understand the following concepts:

- Cisco Unified SRST Gateways and Cisco Unified Communications Manager, page B-13
- Codecs, Port Numbers, and IP Addresses, page B-14
- Multicast MOH Transmission, page B-16
- MOH from a Live Feed, page B-16
- MOH from Flash Files, page B-17

Cisco Unified SRST Gateways and Cisco Unified Communications Manager

Cisco Unified SRST gateways can be configured to multicast Real-Time Transport Protocol (RTP) packets from flash memory during fallback and normal Cisco Unified CM operation. To make this happen, Cisco Unified Communications Manager must be configured for multicast MOH so that the audio packets do not cross the WAN. Instead, audio packets are broadcast from the flash memory of Cisco Unified SRST gateways to the same multicast MOH IP address and port number configured for Cisco Unified Communications Manager multicast MOH. IP phones at remote sites are able to pick up RTP packets that are multicast from the local branch gateways instead of from the central Cisco Unified CM.

Multicast MOH for PSTN callers is supported when the Cisco Unified SRST router is used as the Cisco IOS voice gateway for Cisco Unified CM. In this state the Cisco Unified SRST function of the router remains in standby mode (no phones registered) with call control of the phones and gateway provided by Cisco Unified Communications Manager. This feature does not apply when the Cisco Unified SRST router is in fallback mode (phones are registered to Cisco Unified SRST). Instead, MOH is provided to PSTN callers via a direct internal path rather than through the multicast loopback interface.

Figure 1 shows a sample configuration in which all phones are configured by Cisco Unified Communications Manager to receive multicast MOH through port number 16384 and IP address 239.1.1.1. Cisco Unified CM is configured so that multicast MOH cannot reach the WAN, and local Cisco Unified SRST gateways are configured to send audio packets from their flash files to port number 16384 and IP address 239.1.1.1. Cisco Unified CM and the IP phones are spoofed and behave as if Cisco Unified CM were originating the multicast MOH.

---

**Note**

Phone users at the central site would use multicast MOH from the central site.
Cisco Unified SRST multicast MOH supports G.711 only. Figure 2 shows an example in which G.711 is the only codec used by a central Cisco Unified CM and three branches. In some cases, a Cisco Unified CM system may use additional codecs. For example, for bandwidth savings, Cisco Unified CM may use G.711 for multicast MOH and G.729 for phone conversations.

As shown in the example in Figure 2, IP address 10.1.1.1 and port 1000 are used during phone conversations when G.729 is in use, and IP address 239.1.1.1 and port 16384 are used when a call is placed on hold and G.711 is in use.
Figure 2  
**IP Address and Port Usage for G.711 and G.729 Configuration**

Branch 1 calls Branch 2 (G.729 is used).

![Diagram showing IP Address and Port Usage for G.711 and G.729 Configuration]

Branch 2 places Branch 1 on hold (G.711 is used).

![Diagram showing Branch 2 placing Branch 1 on hold]

Branch 2 takes Branch 1 off hold (G.729 is used).

![Diagram showing Branch 2 taking Branch 1 off hold]

Figure 1 and Figure 2 show all branches using Cisco Unified SRST multicasting MOH. Figure 3 shows a case in which some gateways are configured with Cisco Unified SRST and other gateways are not. When the central site and Branch 3 phone users are put on hold by other IP phones in the Cisco Unified CM system, MOH is originated by Cisco Unified CM. When Branch 1 and Branch 2 phone users are put on hold by other phone users in the Cisco Unified CM system, MOH is originated by the Cisco Unified SRST gateways.
To enable MOH audio packet transmission through two paths, the Cisco Unified CM MOH server must be configured with either one IP address and two different port numbers or one port address and two different IP multicast addresses so that one set of branches can use Cisco Unified SRST multicast MOH and the other can use Cisco Unified CM multicast MOH.

**Multicast MOH Transmission**

If Cisco Unified SRST multicast MOH is supported by all branches in a system, such as in Figure 1, Cisco Unified Communications Manager must be configured to keep all multicast MOH audio packets from reaching the WAN. When there is a mix of Cisco Unified SRST branches, as shown in Figure 3, one set of Cisco Unified Communications Manager MOH audio files must reach the WAN and another set must not. Audio packets from the central Cisco Unified Communications Manager must cross the WAN to reach branches running Cisco Unified Communications Manager. For branches running Cisco Unified SRST, the packets must not reach the WAN. For more information about Multicast MOH, see the “Configuring Cisco Unified SRST for Multicast MOH from an Audio File” section on page B-26.

**MOH from a Live Feed**

MOH live feed provides live feed MOH streams from an audio device connected to an E&M or FXO port to Cisco IP phones in SRST mode. Music from a live feed is from a fixed source and is continuously fed into the MOH playout buffer instead of being read from a flash file.

Cisco Unified SRST is enhanced with the **moh-live** command. The **moh-live** command provides live feed MOH streams from an audio device connected to an E&M or FXO port to Cisco IP phones in SRST mode. Live feed MOH can also be multicast to Cisco IP phones. For more information about Cisco Unified SRST MOH live feed, see the “Configuring Cisco Unified SRST for MOH from a Live Feed” section on page B-36.
MOH from Flash Files

The MOH Multicast from Flash Files feature facilitates the continuous multicast of MOH audio feed from files in the flash memories of Cisco Unified SRST branch office routers during Cisco Unified Communications fallback and normal Cisco Unified Communications service. Multicasting MOH from individual branch routers saves WAN bandwidth by eliminating the need to stream MOH audio from central offices to remote branches.

The MOH Multicast from Flash Files feature can act as a backup mechanism to the MOH live feed feature. Using the Flash to backup the live-feed is the recommend method rather than using just the live feed feature alone.

Cisco Unified Communications Manager MOH audio files must reach the WAN and another set must not. Audio packets from the central Cisco Unified CM must cross the WAN to reach branches running Cisco Unified CM. For branches running Cisco Unified SRST, the packets must not reach the WAN.

Table 1 provides a summary of options for MOH.

<table>
<thead>
<tr>
<th>Audio Source</th>
<th>Description</th>
<th>How to Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash memory</td>
<td>No external audio input is required.</td>
<td>Configuring Cisco Unified SRST for Multicast MOH from an Audio File, page B-26</td>
</tr>
<tr>
<td>Live feed</td>
<td>The multicast audio stream has minimal delay for local IP phones. The MOH stream for PSTN callers is delayed by a few seconds. If the live feed audio input fails, callers on hold hear silence.</td>
<td>Configuring Cisco Unified SRST for MOH from a Live Feed, page B-36</td>
</tr>
<tr>
<td>Live feed and flash memory</td>
<td>The live feed stream has a few seconds of delay for both PSTN and local IP phone callers. The flash MOH acts as backup for the live-feed MoH. We recommend this option if you want live-feed because it provides guaranteed MOH if the live-feed input is not found or fails.</td>
<td>Configuring Cisco Unified SRST for Multicast MOH from an Audio File, page B-26 and Configuring Cisco Unified SRST for MOH from a Live Feed, page B-36</td>
</tr>
</tbody>
</table>
How to Use Cisco Unified SRST Gateways as a Multicast MOH Resource

To use Cisco Unified SRST gateways as a multicast MOH resource, perform the following tasks:

- Configuring Cisco Unified Communications Manager for Cisco Unified SRST Multicast MOH, page B-18
- Configuring Cisco Unified SRST for Multicast MOH from an Audio File, page B-26
- Configuring Cisco Unified SRST for MOH from a Live Feed, page B-36

For Cisco Unified CM 8.0 or later, see the Configuring MOH-groups for Cisco Unified SRST (fallback) section in the Cisco Unified Survivable Remote Site Telephony 8.0 Music On Hold Enhancement document.

Configuring Cisco Unified Communications Manager for Cisco Unified SRST Multicast MOH

The following sections describe the Cisco Unified CM configuration tasks for Cisco Unified SRST multicast MOH:

- Configuring the MOH Audio Source to Enable Multicasting, page B-19
- Enabling Multicast on the Cisco Unified Communications Manager MOH Server and Configuring Port Numbers and IP Addresses, page B-20
- Creating an MRG and an MRGL, Enabling MOH Multicast, and Configuring Gateways, page B-23
- Creating a Region for the MOH Server, page B-25
- Verifying Cisco Unified Communications Manager Multicast MOH, page B-26

To use Cisco Unified SRST gateways as multicast MOH resources, you must configure Cisco Unified Communications Manager to multicast MOH to the required branch sites. To accomplish this, you must configure IP addresses, port numbers, the MOH source, and the MOH audio server.

Even though the MOH routing is set up to prevent the Cisco Unified CM-sourced multicast MOH from actually reaching the WAN and the remote phones, the configured Cisco Unified CM MOH IP port and address information are still used by Cisco Unified CM to tell the phones which multicast IP address to listen to for MOH (for the MOH sourced by SRST).

Configuring the MOH server involves designating a maximum number of hops for the audio source. A configuration of one hop keeps Cisco Unified CM multicast MOH packets from reaching the WAN, thus spoofing Cisco Unified CM and allowing Cisco Unified SRST multicast MOH packets to be sent from Cisco Unified SRST gateways to their component phones. For cases in which Cisco Unified CM multicast must reach gateways that do not run Cisco Unified SRST, use the Cisco IOS ip multicast boundary command to control where multicast packets go.

After the MOH server is configured, the MOH server must be added to a Media Resource Group (MRG); the MRG is added to a Media Resource Group List (MRGL); and the designated Cisco Unified CM branch gateways are configured to use the MRGL.

Five Cisco Unified CM windows are used to configure the MOH server, audio source, MRG, MRGL, and individual gateways. Figure 4 provides an overview of this process.

The last Cisco Unified CM configuration task involves creating an MOH region that assigns MOH G.711 codec usage for the central site or sites and branch office or offices.
Regions specify the codecs that are used for audio and video calls within a region and between existing regions. For information about regions, see the “Region Configuration” section in the *Cisco Unified Communications Manager Administration Guide*. From the *Cisco Unified Communications Manager* documentation directory, click **Maintain and Operate Guides** and select the required Cisco Unified Communications Manager version to locate the administration guide for your version.

**Figure 4 Unified Communications Manager Screens for Configuring Multicast MOH**

Configure MOH Server

Music On Hold (MOH) Audio Source Configuration Screen

Music On Hold (MOH) Server Configuration Screen

Add Server

Media Resource Group Configuration Screen

Add MRG

Media Resource Group Configuration Screen

Phone Configuration Screen

Gateway Configuration Screen

**Configuring the MOH Audio Source to Enable Multicasting**

The MOH audio source is a file from which Cisco Unified CM transmits RTP packets. You can create an audio file or use the default audio file. For Cisco Unified SRST multicast MOH, only one audio source can be used, even if, for example, one out of 500 sites uses Cisco Unified SRST multicast MOH. In addition, all Cisco Unified Communications Manager systems must use the same audio source for user and network MOH because Cisco Unified SRST multicast MOH can stream audio only to a single multicast IP address and port. For Cisco Unified SRST multicast MOH, the Cisco Unified Communications Manager audio source file must be configured for G.711 bandwidth.
How to Use Cisco Unified SRST Gateways as a Multicast MOH Resource

Tip

The simplest way to create an audio source is to use the default audio source.

Whether you use a default Cisco Unified CM MOH audio source or you create one, the MOH audio source must be configured for multicasting in the MOH Audio Source Configuration window.

Note that the MOH Audio Source File Status section shows that the MOH audio source file is configured for four codec formats. If you are planning to use several codecs, ensure that the audio source file accommodates them.

For further information about the creation of an MOH audio source, see the Cisco Unified Communications Manager Administration Guide. From the Cisco Unified Communications Manager documentation directory, click Maintain and Operate Guides and select the required Cisco Unified CM version.

Use this procedure to configure the MOH audio source to enable multicasting and continuous play.

Note

These instructions assume that an MOH audio source file was already created.

Step 1

To enable multicast MOH for the MOH audio source, choose Service > Media Resources > Music On Hold Audio Source to display the MOH Audio Source Configuration window.

Step 2

Double-click the required audio source listed in the MOH Audio Sources column.

Step 3

In the MOH Audio Source Configuration window, check Allow Multicasting.

Step 4

Click Update.

Enabling Multicast on the Cisco Unified Communications Manager MOH Server and Configuring Port Numbers and IP Addresses

Enter a base multicast IP address and port number in the Multicast Audio Source Information section of the MOH Server Configuration window. If you are using Cisco Unified CM multicast MOH and Cisco Unified SRST multicast MOH (see the “Codecs, Port Numbers, and IP Addresses” section on page B-14 and the “Multicast MOH Transmission” section on page B-16), you must select a port and IP address increment method to configure for two sets of port numbers and IP address.

If the Increment Multicast on radio button is set to IP address, each MOH audio source and codec combination is multicast to different IP addresses but uses the same port number. If it is set to Port Number, each MOH audio source and codec combination is multicast to the same IP address but uses different destination port numbers.

Table 2 shows the difference between incrementing on an IP address and incrementing on a port number, using the base IP address of 239.1.1.1 and the base port number of 16384. The table also matches Cisco Unified Communications Manager audio sources and codecs to IP addresses and port numbers.
The lower destination port 16384 is assigned to the first multicast-enabled audio source ID, and the subsequent ports will be assigned to the subsequent multicast-enabled audio sources.

Incrementation is triggered by a change in codec usage. When codec usage changes, a new IP address or port number (depending on the incrementation selected) is assigned to the new codec type and is put into use. The original codec keeps its IP address and port number. For example, as seen in Table 2, if your baseline IP address and port number are 239.1.1.1 and 16384 for a G.711 mu-law codec and the codec usage changes to G.729 (triggering an increment on the port number), the IP address and port number in use changes, or increment, to 239.1.1.1 and 16386. If G.711 usage resumes, the IP address and port number returns to 239.1.1.1 and 16384. If G.729 is in use again, the IP address and port goes back to 239.1.1.1 and 16386, and so forth.

It is important to configure a Cisco Unified CM port number and IP address that use a G.711 audio source for Cisco Unified SRST multicast MOH. If Cisco Unified CM multicast MOH is also being used on gateways that do not have Cisco Unified SRST and use a different codec, such as G.729, ensure that the additional or incremental port number or IP address uses the same audio source as the Cisco Unified SRST gateways and the required codec.

The MOH Server Configuration window is also where the multicast audio source for the MOH server is configured. For Cisco Unified SRST multicast MOH, the Cisco Unified CM MOH server can use only one audio source. An audio source is selected by inputting the audio source’s maximum number of hops.

The Max Hops configuration sets the length of the transmission of the audio source packets. Limiting the number of hops is one way to stop audio packets from reaching the WAN and thus spoofing Cisco Unified Communications Manager so Cisco Unified SRST can multicast MOH. If all of your branches run Cisco Unified SRST, use a low number of hops to prevent audio source packets from crossing the WAN. If your system configuration includes routers that do not run Cisco Unified SRST, enter a high number of hops to allow source packets to cross the WAN. Use the ip multicast bounder and access-list commands to keep resource packets from specific IP addresses from reaching the WAN.

### Table 2

<table>
<thead>
<tr>
<th>Audio Source</th>
<th>Codec</th>
<th>Increment Multicast on IP Address</th>
<th>Increment Multicast on Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Destination IP Address</td>
<td>Destination Port</td>
</tr>
<tr>
<td>1</td>
<td>G.711 mu-law</td>
<td>239.1.1.1 16384</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>G.711 a-law</td>
<td>239.1.1.2 16384</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>G.729</td>
<td>239.1.1.3 16384</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Wideband</td>
<td>239.1.1.4 16384</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>G.711 mu-law</td>
<td>239.1.1.5 16384</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>G.711 a-law</td>
<td>239.1.1.6 16384</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>G.729</td>
<td>239.1.1.7 16384</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Wideband</td>
<td>239.1.1.8 16384</td>
<td></td>
</tr>
</tbody>
</table>
Use this procedure to enable multicast and configure port numbers and IP addresses.

**Step 1**
Enable multicast MOH for Cisco Unified CM.
- Choose **Service > Media Resource > Music On Hold Server**.
- The MOH Server Configuration window appears.
- Call up an existing MOH server by clicking **Find** and double-clicking the required MOH server.
- Whether you are updating an existing MOH server or creating a new one, click **Enable Multicast Audio Sources on this MOH Server**.

**Step 2**
Set the base IP address and port number.
In the MOH Server Configuration window, enter an IP address in the Base Multicast IP Address field and enter a port number in the Base Multicast Port Number field. Ensure that the IP address and port number use the required audio source and codec. See Table 2.

**Step 3**
Select whether Cisco Unified CM increments port numbers or IP addresses.
In the MOH Server Configuration window, in the Increment Multicast on field, choose **Port Number** if you want port numbers to be incremented and the IP address to remain unchanged. Choose **IP Address** if you want IP addresses to be incremented and the port number to remain unchanged.
- If all of your branches run Cisco Unified SRST and thus use G.711 for MOH, use either setting because incrementation does not take place and a selection does not matter.
- If your system configuration includes routers that do not run Cisco Unified SRST and use a different codec, select an incrementation method.

**Note**
If your branches include routers that do not run Cisco Unified SRST and do use G.711, configure separate audio sources: one for the routers that run Cisco Unified SRST and one for the routers that do not.

**Step 4**
Enter a maximum number of hops.
In the MOH Server Configuration window, next to the Audio Source Name field, enter 1 in the Max Hops field if all of your branches run Cisco Unified SRST. If your system configuration includes routers that do not run Cisco Unified SRST, enter 16 in the Max Hops field.

**Step 5**
Use Cisco IOS commands to stop Cisco Unified CM signals from crossing the WAN and reaching Cisco Unified SRST gateways.
If all of your branches run Cisco Unified SRST, skip this step. If your system configuration includes routers that do not run Cisco Unified SRST and use a different codec, enter the following Cisco IOS commands starting from global configuration mode on the central site router:
- **interface {serial | fastethernet} slot/port**
  Enters interface configuration mode, where *slot* is the slot number and *port* is the port number.
- **ip multicast boundary access-list-number**
  Configures an administratively scoped boundary, where *access-list-number* is a number from 1 to 99 that identifies an access list that controls the range of group addresses affected by the boundary.
- **exit**
  Exits interface configuration mode.
d. **access-list access-list-number deny ip-address**

   Configures the access list mechanism for filtering frames by IP address. For the *ip-address* argument, enter the MOH IP address that you want to prevent from going over the WAN. Normally this would be the base IP address entered in Step 2.

   The following is an example configuration:

   ```
   Router(config)# interface serial 0/0
   Router(config-if)# ip multicast boundary 1
   Router(config-if)# exit
   Router(config)# access-list 1 deny 239.1.1.1
   ```

**Creating an MRG and an MRGL, Enabling MOH Multicast, and Configuring Gateways**

The next task involves configuring individual gateways to use an MOH server that can transport the required MOH audio source to their IP phones on hold. This is accomplished by creating a Media Resource Group (MRG). An MRG references media resources, such as MOH servers. The MRG is then added to a Media Resource Group List (MRGL), and the MRGL is added to the phone and gateway configurations.

MRGs are created in the Media Resource Group Configuration window. MRGLs are created in the Media Resource Group List Configuration window. Phones are configured in the Phone Configuration window. Gateways are configured in the Gateway Configuration window.

---

**Note**

The Gateway Configuration window for an H.323 gateway is similar for MGCP gateways.

Add MRGL to a gateway or IP phone configuration by adding the MRGL to a device pool configuration. For further information about device pools, see *Cisco Unified Communications Manager Administration Guide*. From the *Cisco Unified Communications Manager* documentation directory, click **Maintain and Operate Guides** and select the required Cisco Unified CM version.
Use the following procedure to create an MRG and MRGL, to enable MOH multicast, and to configure gateways.

**Step 1** Create an MRG with a multicast MOH media resource.

a. Choose **Service > Media Resource > Media Resource Group.**

b. In the upper-right corner of the window, click the **Add a New Media Resource Group** link. The Media Resource Group Configuration window appears.

c. Complete the Media Resource Group Name field.

d. Complete the Description field.

e. Select a media resource from the Available Media Resources pane. This pane lists the media resources that can be chosen for an MRG and can include the following media resource types:
   - Conference bridges (CFB)
   - Media termination points (MTP)
   - Music-on-hold servers (MOH)
   - Transcoders (XCODE)
   - Annunciator (ANN)

Music-on-hold servers that are configured for multicast are labeled as (MOH) [Multicast].

f. Click the down arrow so that the selected media resource moves to the Selected Media Resources pane.

g. Click **Insert.**

**Step 2** Create an MRGL that contains the newly created MRG.

a. Choose **Service > Media Resource > Media Resource Group List.**

b. In the upper-right corner of the window, click the **Add a New Media Resource Group List** link. The Media Resource Group List Configuration window appears.

c. Complete the Media Resource Group List Name field.

d. In the Available Media Resource Groups pane, select the MRG that you just created.

e. Add the MRG to the Selected Media Resource Groups pane by clicking the down arrow. After a media resource group is added, its name moves to the Selected Media Resource Groups pane.

f. Click **Insert.**

**Step 3** Add the MRGL to the required IP phones.

a. Choose **Device > Phone** to display the Find and List Phones window.

b. Click **Find** to display a list of phones.

c. Double-click the device name of the phone that you want to update.

d. Complete the Media Resource Group List field by choosing the required MRGL from the drop-down menu.

e. Click **Update.**

**Step 4** Add the MRGL to the required gateway.

a. Choose **Device > Gateway** to display the Find and List Gateways window.

b. Click **Find** to display a list of gateways.
c. Double-click the device name of the gateway that you want to update.

d. If the gateway is H.323, complete the Media Resource Group List field by choosing the required MRGL from the drop-down menu.

e. Click Update.

Creating a Region for the MOH Server

To ensure that the MOH server uses G.711 for Cisco Unified SRST gateways, you must create a separate region for the MOH server. For more information about codecs, see the “Codecs, Port Numbers, and IP Addresses” section on page B-14. For information about regions, see Cisco Unified Communications Manager Administration Guide. From the Cisco Unified Communications Manager documentation directory, click Maintain and Operate Guides and select the required Cisco Unified Communications Manager version.

Configure the Region Configuration window. If the Cisco Unified CM system uses G.711 only, all of the central sites and their constituent branches for the MOH region must be set to G.711. If a Cisco Unified CM system has a combination of branches that do and do not run Cisco Unified SRST multicast MOH and the branches that do not run Cisco Unified SRST require a different codec for Cisco Unified Communications Manager multicast MOH, they must be configured accordingly.

A Region Configuration window where the “MOH Server” region is configured to use the G.711 and G.729 codecs might look like this:

- G.711 is used for Branch 1 because its gateway is configured to run Cisco Unified SRST multicast MOH, which requires G.711.
- G.729 is used for Branch 2 because its gateway does not run Cisco Unified SRST and it is configured to use a port and IP address that use G.729.
- G.711 is configured for the central site and the MOH server region.

Use the following procedure to create a region for the MOH server.

Step 1 Create an MOH server region.

a. Choose System > Region.

b. In the upper-right corner of the window, click Add a New Region. The Region Configuration window appears.

c. In the Region Name field, enter the name that you want to assign to the new region and click Insert.

d. If other regions were created, a list of regions appear. Use the drop-down list boxes to choose the audio codec to use for calls between the new region and existing regions. The audio codec determines the type of compression and the maximum amount of bandwidth that is allocated for these calls.

e. In addition to other regions, the newly created region appears in the list. Use its drop-down box to choose the codec for use within the new region.

f. Click Update.

Step 2 Create other regions as needed for different codecs.
Verifying Cisco Unified Communications Manager Multicast MOH

The Cisco Unified CM multicast MOH configuration must run correctly for Cisco Unified SRST multicast MOH to work. Verification of Cisco Unified Communications Manager multicast MOH differs for configurations using a WAN with multicast enabled and a WAN with multicast disabled.

You must verify that the Cisco Unified CM multicast MOH is provided through multicasting and not unicasting. Because unicast MOH is enabled by default, it is easy to mistakenly conclude that multicast MOH is working when it is not.

Step 1
Verify that Cisco Unified CM system’s multicast MOH is heard on a remote gateway.

a. If multicast is enabled on the WAN, make sure that the number of hops configured on the Cisco Unified Communications Manager MOH server is sufficient to allow audio packets to reach the remote site (see the “Enabling Multicast on the Cisco Unified Communications Manager MOH Server and Configuring Port Numbers and IP Addresses” section on page B-20). Then call an IP phone on a remote gateway, place the call on hold, and verify that MOH is heard.

b. If multicast is not enabled on the WAN, place an IP phone on the same subnet as the Cisco Unified Communications Manager MOH server and verify that MOH can be heard. Because the IP phone and the MOH server are on the same subnet, no multicast routing capabilities in the network are required.

Step 2
Verify that the Cisco Unified CM system’s MOH is multicast, not unicast.

a. From Microsoft Windows, select Start > Programs > Administrative Tools > Performance.

b. In the Performance window, click the + (plus) icon located at the top of the right pane.

c. In the Add Counters window, select Cisco MOH Device.

d. In the Performance window, you can monitor the MOHMulticastResourceActive and MOHUnicastResourceActive counters to check on multicast activity.

Configuring Cisco Unified SRST for Multicast MOH from an Audio File

Note
Use the steps in this section only when you are using Microsoft Windows to run Cisco Unified Communications Manager version 4.3 or below. Use the RTMT (Real-Time Monitoring Tool) in Cisco Unified Communications Manager version 5.0 and later versions on the Linux operating system to monitor MOH activity in Cisco Unified CM version. See Cisco Unified Communications Serviceability System Guide, Release 4.0(1) for more information about RTMT.

Use the following procedures to configure Cisco Unified SRST for multicast MOH from an audio file.

- Enabling Multicast MOH on the Cisco Unified SRST Gateway, page B-27
- Verifying Basic Cisco Unified SRST Multicast MOH Streaming, page B-31
- Verifying Cisco Unified SRST MOH to PSTN, page B-32
- Verifying Cisco Unified SRST Multicast MOH to IP Phones, page B-36
Prerequisites

- The Cisco Unified SRST gateways must run Cisco IOS Release 12.2(15)ZJ2 or a later release.
- The flash memory in each of the Cisco Unified SRST gateways must have an MOH audio file. The MOH file can be in .wav or .au file format, but must contain 8-bit 8-kHz data, such as an a-law or mu-law data format. A known working MOH audio file (music-on-hold.au) is included in the program .zip files that can be downloaded from http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key. Or the music-on-hold.au file can be downloaded from http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp and copied to the flash memory on your Cisco Unified SRST router.

  Note  The MOH file packaged with the SRST software is completely royalty free.

- For Cisco Unified CM versions 4.3 or earlier versions running on Windows, download MOH files by copying one of the MOH files, such as SampleAudioSource.ULAW.wav, from C:\Program Files\Cisco\MOH on Cisco Unified CM.

  Note  During the copying process, four files are added to each router’s flash automatically. One of the files must use a mu-law format as indicated by the extension.ULAW.wav.

- You must configure a loopback interface and include its IP addresses in the Cisco Unified SRST multicast MOH configuration. This configuration allows multicast MOH to be heard on POTS ports on the gateway. The loopback interface does not have to bind to either H.323 or MGCP.

- Configure at least one ephone and directory number (DN), even if the gateway is not used for Cisco Unified SRST. Cisco Unified SRST multicast MOH streaming never starts without an ephone and directory number.

Enabling Multicast MOH on the Cisco Unified SRST Gateway

No multicast MOH routing configuration is required for Cisco Unified SRST gateways because each Cisco Unified SRST gateway is configured to act as a host running an application that streams multicast MOH packets from the network. The multicast moh command declares the Cisco Unified Communications Manager multicast MOH address and port number and allows Cisco Unified SRST gateways to route MOH from flash memory to up to four IP addresses. If no route IP addresses are configured, the flash MOH is sent through the IP address configured in the Cisco Unified SRST ip source-address command.

SUMMARY STEPS

1. ccm-manager music-on-hold
2. interface loopback number
3. ip address ip-address mask
4. exit
5. interface fastethernet slot/port
6. ip address ip-address mask
7. exit
8. call-manager-fallback
9. `ip source-address ip-address [port port]`
10. `max-ephones max-phones`
11. `max-dn max-directory-number`
12. `moh filename`
13. `multicasting-enabled`
14. `multicast moh multicast-address port port [route ip-address-list]`
15. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | ccm-manager music-on-hold
| Example: | Enables the multicast MOH feature on a voice gateway. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** | interface loopback number
| Example: | Configures an interface type and enters the interface configuration mode. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** | ip address ip-address mask
| Example: | Sets a primary IP address for an interface. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 4** | exit
| Example: | Exits interface configuration mode. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | interface fastethernet slot/port
| Example: | (Optional if the `route` keyword is not used in the `multicast moh` command. See Step 9 and Step 13.) Configures an interface type and enters interface configuration mode. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 6** | ip address ip-address mask
| Example: | (Optional if the `route` keyword is not used in the `multicast moh` command. See Step 9 and Step 13.) Sets a primary IP address for an interface. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 7** | exit
| Example: | (Optional if the `route` keyword is not used in the `multicast moh` command. See Step 9 and Step 13.) Exits interface configuration mode. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 8** | call-manager-fallback
| Example: | Enters call-manager-fallback configuration mode. |

Example:

```
Router(config)# call-manager-fallback
```

---

Cisco Unified SCCP and SIP SRST System Administrator Guide

B-28
### Command or Action

**Step 9**  
`ip source-address ip-address [port port]`

**Example:**
Router(config-cm-fallback)# ip source-address 172.21.51.143 port 2000

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional if the <code>route</code> keyword is not used in the <code>multicast moh</code> command. See Step 13.) Enables a router to receive messages from Cisco Unified IP phones through the specified IP addresses and ports.</td>
</tr>
<tr>
<td>- <code>ip-address</code>—The pre-existing router IP address, typically one of the addresses of the Ethernet port of the router.</td>
</tr>
<tr>
<td>- <code>port</code>—(Optional) The port to which the gateway router connects to receive messages from the Cisco Unified IP phones. The port number range is from 2000 to 9999. The default port number is 2000.</td>
</tr>
</tbody>
</table>

**Step 10**  
`max-ephones max-phones`

**Example:**
Router(config-cm-fallback)# max-ephones 1

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the maximum number of Cisco Unified IP phones that can be supported by a router.</td>
</tr>
<tr>
<td>- <code>max-phones</code>—Maximum number of Cisco IP phones supported by the router. The maximum number is platform-dependent. The default is 0.</td>
</tr>
</tbody>
</table>

**Step 11**  
`max-dn max-directory-number`

**Example:**
Router(config-cm-fallback)# max-dn 1

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the maximum possible number of virtual voice ports that can be supported by a router.</td>
</tr>
<tr>
<td>- <code>max-directory-number</code>—Maximum number of directory numbers or virtual voice ports supported by the router. The maximum possible number is platform-dependent. The default is 0.</td>
</tr>
</tbody>
</table>

**Step 12**  
`moh filename`

**Example:**
Router(config-cm-fallback)# moh music-on-hold.au

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables use of an MOH file.</td>
</tr>
<tr>
<td>- <code>filename</code>—Filename of the music file. The music file must reside in flash memory.</td>
</tr>
</tbody>
</table>

**Step 13**  
`multicasting-enabled`

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects the multicast-enabled MOH audio source in the User Hold MOH Audio Source field on the Phone Configuration page in Cisco Unified CM Administration GUI.</td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 14

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>multicast moh multicast-address port port [route ip-address-list]</code></td>
<td>Enables multicast of MOH from a branch office flash MOH file to IP phones in the branch office.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-cm-fallback)# multicast moh 239.1.1.1 port 16386 route 239.1.1.2 239.1.1.3 239.1.1.4 239.1.1.5
```

- `multicast-address` and `port port`—Declares the IP address and port number of MOH packets that are to be multicast. The multicast IP address and port must match the IP address and the port number that Cisco Unified CM is configured to use for multicast MOH. If you are using different codecs for MOH, these might not be the base IP address and port, instead an incremented IP address or port number. See the “Configuring the MOH Audio Source to Enable Multicasting” section on page B-19. If you have multiple audio sources configured on Cisco Unified CM, ensure that you are using the audio sources’s correct IP address and port number.
- `route`—(Optional) List of explicit router interfaces for the IP multicast packets.
- `ip-address-list`—(Optional) List of up to four explicit routes for multicast MOH. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the `ip source-address` command.

#### Step 15

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-cm-fallback)# exit
```
Verifying Basic Cisco Unified SRST Multicast MOH Streaming

Use the following procedure to verify that multicast MOH packets are configured with the `multicast moh` command.

**SUMMARY STEPS**

1. `debug ephone moh`
2. `show interfaces fastethernet`
3. `show ephone summary`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>debug ephone moh</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# <code>debug ephone moh</code></td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>MOH route If FastEthernet0/0 ETHERNET 172.21.51.143</td>
<td></td>
</tr>
<tr>
<td>via ARP</td>
<td></td>
</tr>
<tr>
<td>MOH route If Loopback0 46 172.21.51.98 via</td>
<td></td>
</tr>
<tr>
<td>172.21.51.98</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>This command sets debugging for MOH. You can use this command to show that the Cisco Unified SRST gateway is multicasting MOH out of Loopback 0 and Fast Ethernet 0/0.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** `show interfaces fastethernet` |         |
| Example:                                 |         |
| Router# `show interfaces fastethernet 0/0` |         |
| !                                        |         |
| 30 second output rate 86000 bits/sec, 50 packets/sec |         |
| !                                        |         |
| Use this command to confirm that the interface output rates match one G.711 stream, which the `show interfaces fastethernet` output displays as 50 packets/sec and 80 kbps or more. |

| **Step 3** `show ephone summary`         |         |
| Example:                                 |         |
| Router# `show ephone summary`            |         |
| !                                        |         |
| File music-on-hold.au type AU            |         |
| Media_Payload_G.711Ulaw64k 160 bytes     |         |
| !                                        |         |
| Use this command to verify that the Cisco IOS software was able to read the MOH audio file successfully. |

**Troubleshooting Tips**

The `show ephone summary` output should show a file type as either .au or .wav. If `INVALID` appears, an error exists.

Router# `show ephone summary`

! File music-on-hold.au type INVALID Media_Payload_G.711Ulaw64k 160 bytes651-
An invalid output might be caused by the order in which the Cisco Unified SRST configuration commands are entered. Use the `no call-manager-fallback` command and reenter the multicast MOH commands. Rebooting may also clear the error.

**Verifying Cisco Unified SRST MOH to PSTN**

Use the following procedure to verify Cisco Unified CM control of MOH (the WAN link is up) and that multicast MOH packets transmit over a public switched telephone network (PSTN).

**SUMMARY STEPS**

1. Verify that a PSTN caller hears MOH when placed on hold by an IP phone caller.
2. `show ccm-manager music-on-hold`
3. `debug h245 asn`
4. `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></td>
<td>Verify that a PSTN caller hears MOH when placed on hold by an IP phone caller.</td>
</tr>
<tr>
<td></td>
<td>Use a Cisco Unified SRST gateway IP phone to call a PSTN phone, and put the PSTN caller on hold. The PSTN caller should hear MOH.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Use this command to verify that the MOH is multicast if you are using Windows and Cisco Unified CM version 4.3 or an earlier version. Note that the <code>show ccm-manager music-on-hold</code> command displays information about PSTN connections on hold only. It does not display information about multicast streams going to IP phones on hold. The following is an example of <code>show ccm-manager music-on-hold</code> command output. If the PSTN caller hears MOH, and the <code>show ccm-manager music-on-hold</code> command displays no active multicast streams, the MOH is unicast. Confirm this by checking the MOH performance counters as discussed in the “Verifying Cisco Unified Communications Manager Multicast MOH” section on page B-26.</td>
</tr>
<tr>
<td><code>show ccm-manager music-on-hold</code></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router# show ccm-manager music-on-hold</td>
</tr>
<tr>
<td></td>
<td>Current active multicast sessions : 1</td>
</tr>
<tr>
<td></td>
<td>Multicast RTP port Packets Call Codec Incoming Address number in/out id Interface</td>
</tr>
<tr>
<td></td>
<td>==========================================================================</td>
</tr>
<tr>
<td></td>
<td>239.1.1.1 16384 326/326 42 G.711ulaw Lo0</td>
</tr>
</tbody>
</table>
**Troubleshooting Tips**

- If the PSTN caller hears tone on hold (TOH) instead of MOH, two problems are probable:
  - Cisco Unified CM has failed to activate MOH and has used TOH as a fallback. To verify that this is the case, see the “Verifying Cisco Unified Communications Manager Multicast MOH” section on page B-26.
  - Cisco Unified CM does not have the appropriate MOH resource available. Use the `show ccm-manager music-on-hold` command to find out if the MOH resource is the problem.

---

**Step 3**

```plaintext
debug h245 asn
```

**Example:**

Router# debug h245 asn

```
*Mar 1 04:20:19.227: H245 MSC INCOMING PDU ::= value MultimediaSystemControlMessage ::= response :
openLogicalChannelAck :
  { forwardLogicalChannelNumber 6
forwardMultiplexAckParameters h2250LogicalChannelAckParameters :
  { sessionID 1
mediaChannel unicastAddress : iAddress :
  { network 'EF010101'H
tsapIdentifier 16384
  }
mediaControlChannel unicastAddress : iAddress :
  { network 'EF010101'H
tsapIdentifier 16385
  }
}
}
```

Use this command if H.323 is being used and no multicast address appears in the `show ccm-manager music-on-hold` command output to verify the H.323 handshaking between Cisco Unified Communications Manager and the Cisco Unified SRST gateway. When a PSTN caller is placed on hold, Cisco Unified Communications Manager sends an H.245 closeLogicalChannel, followed by an openLogicalChannel. Verify that the final openLogicalChannelAck from Cisco Unified Communications Manager to the Cisco Unified SRST gateway contains the expected multicast IP address and port number. In the following example, the IP address is EF010101 (239.1.1.1) and the port number is 16384.

**Step 4**

```plaintext
show call active voice
```

**Example:**

Router# show call active voice | include RemoteMedia

```
RemoteMediaIPAddress=239.1.1.1
RemoteMediaPort=16384
```

Use this command with the `debug h245 asn` command to further verify the H.323 handshaking between Cisco Unified Communications Manager and the Cisco Unified SRST gateway.

The IP address and port number displayed must match the IP address and port number displayed by the `debug h245 asn` command. If the RemoteMediaIPAddress field displays 0.0.0.0, you probably have encountered caveat CSCdz00697. For more information, see the Cisco Bug ToolKit and the “Restrictions for Using Cisco Unified SRST Gateways as a Multicast MOH Resource” section on page B-12.
The `show ccm-manager music-on-hold` command displays information about PSTN connections on hold only. It does not display information about multicast streams going to IP phones on hold.

```
Router# show ccm-manager music-on-hold
```

```
Current active multicast sessions : 1
Multicast   RTP port  Packets    Call  Codec  Incoming
Address     number    in/out    id    Interface
===================================================================
239.1.1.1    16384     326/326   42    G.711ulaw Lo0*
```

If no MOH streams are shown (that is, there are no rows of data beneath the columns), Cisco Unified Communications Manager was not correctly configured to provide the Cisco Unified SRST gateway with MOH. Configuration errors might include that the required codec has not been enabled on Cisco Unified Communications Manager (check the service parameters) and that no MRGL was assigned to the gateway, or, if one was assigned, it has insufficient resources. Check Cisco Intrusion Detection System (Cisco IDS) Event Viewer for error messages.

- If the POTS caller on hold does not hear a sound, Cisco Unified CM has successfully completed the multicast MOH handshaking with the Cisco Unified SRST gateway, and the gateway is failing to pick up the locally generated multicast RTP stream. Use the `show ccm-manager music-on-hold` command to investigate.

```
Router# show ccm-manager music-on-hold
```

```
Current active multicast sessions : 1
Multicast   RTP port  Packets    Call  Codec  Incoming
Address     number    in/out    id    Interface
===================================================================
239.1.1.1    16384     326/326   42    G.711ulaw Lo0*  
```

- If no MOH streams are shown, Cisco Unified CM was not correctly set up to provide the Cisco Unified SRST gateway with MOH. A typical error is that Cisco Unified Communications Manager was not configured with an appropriate MOH resource. The configuration error might be that the required codec has not been enabled on Cisco Unified CM (check the service parameters) or that no MRGL was assigned to the gateway, or, if one is assigned, it has insufficient resources. Check the IDS Event Viewer for error messages.

- Verify that the multicast address and RTP port number shown in the `show ccm-manager music-on-hold` command output match the `multicast-address` and `port` arguments in the `moh multicast` command configuration.

- Verify that the Packets in/out field shows a count that is incrementing. Repeat the `show ccm-manager music-on-hold` command to verify that the Packets in/out counters are incrementing.

- Verify that the codec field matches the codec type of the audio file stored in the Cisco Unified SRST gateway’s flash memory. If another codec value besides G.711 mu-law or G.711 a-law appears in the `show ccm-manager music-on-hold` command output, review the Cisco Unified CM region for incorrect codec configuration. See the “Creating a Region for the MOH Server” section on page B-25.
The Incoming Interface field shows where the Cisco Unified SRST gateway is to receive the multicast MOH packets. An interface must be listed and it must be one of the interfaces included in the `multicast moh` command or the default IP source address, which is configured with the `ip source-address` command.

For more information, see Step 9 in the “Enabling Multicast MOH on the Cisco Unified SRST Gateway” section on page B-27.
Verifying Cisco Unified SRST Multicast MOH to IP Phones

To verify that Cisco Unified CM is signaling the IP phone to receive Cisco Unified SRST multicast MOH correctly, perform the following steps.

**Step 1**
Verify that an IP phone caller hears MOH when placed on hold by an IP phone caller.
Use an IP phone to call a second IP phone, and put the second caller on hold. The second caller should hear MOH.

**Step 2**
Check the MOHMulticastResourceActive and MOHUnicastResourceActive counters.
Use the Performance window to check the MOHMulticastResourceActive and MOHUnicastResourceActive counters under the Cisco MOH Device performance object. See Step 2 in the “Verifying Cisco Unified Communications Manager Multicast MOH” section on page B-26. For Cisco Unified SRST multicasting MOH to work, the multicast counter must increment.

**Troubleshooting Tips**

If no MOH is heard and the Cisco Unified SRST MOH signaling is multicasting, connect a sniffer to the PC port on the back of IP phone. If the IP phone and Cisco Unified SRST gateway are connected to the same subnet, multicast RTP packets must be detected at all times, even when the IP phone was not placed on hold. If the IP phone and the Cisco Unified SRST gateway are not connected to the same subnet, multicast RTP packets are detected only when the IP phone is placed on hold and sends an Internet Group Management Protocol (IGMP) Join to the closest router.

**Configuring Cisco Unified SRST for MOH from a Live Feed**

The following sections describe the configuration tasks for Cisco Unified SRST MOH live feed:

- Prerequisites, page B-37
- Restrictions, page B-37
- Setting Up the Voice Port on the Cisco Unified SRST Gateway, page B-37
- Setting Up the Directory Numbers on the Cisco Unified SRST Gateway, page B-39
- Establishing the MOH Feed, page B-39
- Verifying Cisco Unified SRST MOH Live Feed, page B-41

To configure MOH from a live feed, establish a voice port and dial peer for the call and then create a “dummy” phone or directory number. The dummy number allows for making and receiving calls, and the number is not assigned to a physical phone. It is that number that the MOH system autodials to establish the MOH feed.

The **moh-live** command allocates one of the virtual voice ports from the pool of virtual voice ports created by the **max-dn** command. The virtual voice port places an outgoing call to the dummy number; that is, the directory number specified in the **moh-live** command. The audio stream obtained from the MOH call provides the music-on-hold audio stream.

We recommend that the interface for live-feed MOH is an analog E&M port because it requires the minimum number of external components. Connect a line-level audio feed (standard audio jack) directly to pins 3 and 6 of an E&M RJ-45 connector. The E&M WAN interface card (WIC) has a built-in audio transformer that provides appropriate electrical isolation for the external audio source. (An audio
connection on an E&M port does not require loop current.) The **signal immediate** and **auto-cut-through** commands disable E&M signaling on this voice port. A G.711 audio packet stream is generated by a digital signal processor (DSP) on the E&M port.

In Cisco IOS Release 12.4(15)T and later releases, you can directly connect a live-feed source to an FXO port if the **signal loop-start live-feed** command is configured on the voice port; otherwise, the port must connect through an external third-party adapter to provide a battery feed. An external adapter must supply normal telephone company (telco) battery voltage with the correct polarity to the tip and ring leads of the FXO port and it must provide transformer-based isolation between the external audio source and the tip and ring leads of the FXO port.

Music from a live feed is continuously fed into the MOH playout buffer instead of being read from a flash file, so there is typically a 2-second delay. An outbound call to an MOH live-feed source is attempted (or reattempted) every 30 seconds until the connection is made by the directory number that was configured for MOH. If the live-feed source is shut down for any reason, the flash memory source automatically activates.

A live-feed MOH connection is established as an automatically connected voice call that is made by the Cisco Unified SRST MOH system itself or by an external source directly calling in to the live-feed MOH port. An MOH call can be from or to the PSTN or can proceed via VoIP with voice activity detection (VAD) disabled. The call is assumed to be an incoming call unless the **out-call** keyword is used with the **moh-live** command during configuration.

The Cisco Unified SRST router uses the audio stream from the call as the source for the MOH stream, displacing any audio stream that is available from a flash file. An example of an MOH stream received over an incoming call is an external H.323-based server device that calls the directory number to deliver an audio stream to the Cisco Unified SRST router.

**Prerequisites**

Cisco Unified SRST for multicast MOH, as described in the “Configuring Cisco Unified SRST for Multicast MOH from an Audio File” section on page B-26, is not required for the MOH live-feed configuration. However, MOH live feed is designed to work in conjunction with multicast MOH.

**Restrictions**

- An FXO port can be used for a live feed if the port is supplied with an external third-party adapter to provide a battery feed.
- An FXS port cannot be used for a live feed.
- For a live feed from VoIP, VAD must be disabled.
- MOH is supplied to PSTN and VoIP G.711 calls. Some versions of Cisco Unified SRST provide MOH to local phones. On Cisco Unified SRST that do not support MOH for local IP phones, callers hear a repeating tone on hold for reassurance that they are still connected.
- Conditions may occur within your network that is caused by brief spikes of a higher CPU usage. Small spikes in CPU usage can temporarily affect the quality of the MOH heard by parties connected via TDM (FXO / PRI / S) interfaces.

**Setting Up the Voice Port on the Cisco Unified SRST Gateway**

Use the following procedure to activate MOH from a live feed and to set up and connect the physical voice port.
SUMMARY STEPS

1. voice-port port
2. input gain decibels
3. auto-cut-through (E&M only)
4. operation 4-wire (E&M only)
5. signal immediate (E&M only)
6. no shutdown
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> voice-port port</td>
<td>Enters voice-port configuration mode to set up the physical voice port. To find the correct definition of the port argument for your router, see Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config)# voice-port 1/1/0</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong> input gain decibels</td>
<td>Specifies, in decibels, the amount of gain to be inserted at the receiver side of the interface. Acceptable values are integers from –6 to 14.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-voice-port)# input gain 0</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong> auto-cut-through</td>
<td>(E&amp;M ports only) Enables call completion when a PBX does not provide an M-lead response. MOH requires that you use this command with E&amp;M ports.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-voiceport)# auto-cut-through</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong> operation 4-wire</td>
<td>(E&amp;M ports only) Selects the 4-wire cabling scheme. MOH requires that you specify 4-wire operation with this command for E&amp;M ports.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-voiceport)# operation 4-wire</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong> signal immediate</td>
<td>(E&amp;M ports only) For E&amp;M tie trunk interfaces, directs the calling side to seize a line by going off-hook on its E-lead and to send address information as DTMF digits.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-voiceport)# signal immediate</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong> no shutdown</td>
<td>Activates the voice port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-voiceport)# no shutdown</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits voice-port configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-voiceport)# exit</strong></td>
</tr>
</tbody>
</table>
Setting Up the Directory Numbers on the Cisco Unified SRST Gateway

After setting up the voice port, create a dial peer and give the voice port a directory number with the `destination-pattern` command. The directory number is the number that the system uses to access the MOH.

**SUMMARY STEPS**

1. `dial-peer voice tag pots`
2. `destination-pattern string`
3. `port port`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>dial-peer voice tag pots</code></td>
<td>Enters dial-peer configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 7777 pots</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>destination-pattern string</code></td>
<td>Specifies the directory number that the system uses to create MOH. This command specifies either the prefix or the full E.164 telephone number to be used for a dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# destination-pattern 7777</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>port port</code></td>
<td>Associates the dial peer with the voice port that was specified in the “Setting Up the Voice Port on the Cisco Unified SRST Gateway” section on page B-37.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# port 1/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>exit</code></td>
<td>Exits dial-peer configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Establishing the MOH Feed

Use the following procedure to establish the MOH feed and connect the music source, such as a CD player, to autodial the directory number.

**SUMMARY STEPS**

1. `call-manager-fallback`
2. `max-dn max-directory-number`
3. `multicast moh multicast-address port port [route ip-address-list]`
4. `moh-live dn-number calling-number out-call outcall-number`
5. `exit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> max-dn max-directory-number</td>
<td>Sets the maximum possible number of virtual voice ports that can be supported by a router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# max-dn 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> multicast moh multicast-address port port [route ip-address-list]</td>
<td>Enables multicast of MOH from a branch office flash MOH file to IP phones in the branch office.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# multicast moh 239.1.1.1 port 16386 route 239.1.1.2 239.1.1.3 239.1.1.4 239.1.1.5</td>
<td></td>
</tr>
</tbody>
</table>

**Note** This command must be used to source live feed MOH to multicast Cisco Unified CM mode. It is not required in strict SRST mode.

- **multicast-address and port port**—Declares the IP address and port number of MOH packets that are to be multicast. The multicast IP address and port must match the IP address and the port number that Cisco Unified Communications Manager is configured to use for multicast MOH. If you are using different codecs for MOH, these might not be the base IP address and port, but an incremented IP address or port number. See the “Configuring the MOH Audio Source to Enable Multicasting” section on page B-19. If you have multiple audio sources configured on Cisco Unified CM, ensure that you are using the audio sources’ correct IP address and port number.

- **route ip-address-list**—(Optional) Declares the IP address or addresses from which the flash MOH packets can be transmitted. A maximum of four IP address entries are allowed. If a **route** keyword is not configured, the Cisco Unified SRST system uses the **ip source-address** command value configured for Cisco Unified SRST.
To verify MOH live feed, use the `debug ephone moh` command and the other commands described in the “Verifying Basic Cisco Unified SRST Multicast MOH Streaming” section on page B-31.

### Configurations Examples for Cisco Unified SRST Gateways

This section provides the following configuration examples for Cisco Unified SRST gateways:

- MOH Routed to Two IP Addresses: Example, page B-41
- MOH Live Feed: Example, page B-42

### MOH Routed to Two IP Addresses: Example

The following example declares the Cisco Unified CM multicast MOH IP address 239.1.1.1 and port number 16384 and streams music-on-hold.au audio file packets out the interfaces that are configured with the IP addresses 10.1.1.1 and 172.21.51.143:

```
ccm-manager music-on-hold
interface Loopback0
  ip address 10.1.1.1. 255.255.255.255
interface FastEthernet0/0
  ip address 172.21.51.143 255.255.255.192
call-manager-fallback
  ip source-address 172.21.51.143 port 2000
  max-ephones 1
  max-dn 1
  moh music-on-hold.au
```

#### Step 4

**moh-live dn-number calling-number out-call outcall-number**

**Example:**
```
Router(config-cm-fallback)# moh-live dn-number 3333 out-call 7777
```

Specifies that this telephone number is to be used for an outgoing call that is to be the source for an MOH stream.

- **dn-number calling-number**—Sets the MOH telephone number. The `calling-number` argument is a sequence of digits that represent a telephone number.
- **out-call outcall-number**—Indicates that the router is calling out for a live feed that is to be used for MOH and specifies the number to be called. The `outcall-number` argument is a sequence of digits that represent a telephone number, typically of an E&M port.

The `outcall` keyword makes a connection to the local router voice port that was specified in the “Setting Up the Voice Port on the Cisco Unified SRST Gateway” section on page B-37.

#### Step 5

**exit**

**Example:**
```
Router(config-cm-fallback)# exit
```

Exits call-manager-fallback configuration mode.

### Verifying Cisco Unified SRST MOH Live Feed

To verify MOH live feed, use the `debug ephone moh` command and the other commands described in the “Verifying Basic Cisco Unified SRST Multicast MOH Streaming” section on page B-31.
multicast moh 239.1.1.1 port 16384 route 172.21.51.143 10.1.1.1

Note

The multicast IP address and port must match the IP address and the port number that Cisco Unified CM is configured to use for multicast MOH. If you are using different codecs for MOH, these might not be the base IP address and port, but an incremented IP address or port number. See the “Configuring the MOH Audio Source to Enable Multicasting” section on page B-19. If you have multiple audio sources configured on Cisco Unified CM, ensure that you are using the audio source’s correct IP address and port number.

MOH Live Feed: Example

The following example configures MOH from a live feed. Note that the dial peer references the E&M port that was set with the voice-port command and that the dial peer number (7777) matches the outcall number configured with the out-call keyword of the moh-live command.

voice-port 1/0/0
    input gain 3
    auto-cut-through
    operation 4-wire
    signal immediate

!
dial-peer voice 7777 pots
    destination-pattern 7777
    port 2/0/0
! !
call-manager-fallback
    max-conferences 8
    max-dn 1
    moh-live dn-number 3333 out-call 7777
! !

Feature Information for Cisco Unified SRST as a Multicast MOH Resource

Table 3 lists the enhancements to the Cisco Unified SRST as a Multicast MOH Resource feature by version.

To determine hardware and software compatibility, see the Cisco Unified CM Compatibility Information page at the following URL:

See also the Cisco Unified CM Documentation Roadmaps at the following URL:

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS 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 3 lists the Cisco Unified SRST version that introduced support for a given feature. Unless noted otherwise, subsequent versions of Cisco Unified SRST software also support that feature.

**Table 3 Feature Information for Cisco Unified SRST as a Multicast MOH Resource**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified SRST as a Multicast MOH Resource</td>
<td>3.0</td>
<td>The MOH-live feature was added.</td>
</tr>
</tbody>
</table>

**Where to Go Next**

For additional information, see the “Additional References” section on page 1-29 in the “Cisco Unified SRST Feature Overview” section on page 1-1 chapter.