Cisco Unified SRST System Administrator Guide (All Versions)

July 11, 2008

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

Cisco Unified SRST System Administrator Guide

CONTENTS

Cisco Unified Survivable Remote Site Telephony Feature Roadmap

Revised: July 11, 2008

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

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

Table 1 Cisco Unified SRST Configuration Sequence

Chapter or Appendix	Description
Overview of Cisco Unified SRST	Provides a summary of SRST. This chapter includes the following sections: • Cisco Unified SRST Description, page 33 • Support for Cisco Unified IP Phones, Platforms, Cisco Unified Communications Manager, Signals, Languages, and Switches, page 37 • Prerequisites for Configuring Cisco Unified SRST, page 41 • Restrictions for Configuring Cisco Unified SRST, page 43 • Additional References, page 46
Setting Up the Network	Describes how to set up a Cisco Unified SRST system to communicate with your network. This chapter includes the following tasks: • Enabling IP Routing, page 52 • Configuring DHCP for Cisco Unified SRST Phones, page 58 • Specifying Keepalive Intervals, page 61 • Configuring Cisco Unified SRST to Support Phone Functions, page 62 • Verifying That Cisco Unified SRST Is Enabled, page 64
Setting Up Cisco Unified IP Phones	Describes how to set up the basic Cisco Unified SRST phone configuration. This chapter includes the following tasks: • Configuring IP Phone Clock, Date, and Time Formats, page 68 • Configuring IP Phone Language Display, page 69 • Configuring Customized System Messages for Cisco Unified IP Phones, page 70 • Configuring a Secondary Dial Tone, page 72 • Configuring Dual-Line Phones, page 72
Setting Up Call Handling	Describes how to configure incoming and outgoing calls. This chapter includes the following tasks: • Configuring Incoming Calls, page 79 • Configuring Outgoing Calls, page 98
Configuring Additional Call Features	Describes how to configure optional system and phone parameters. This chapter includes the following tasks: • Enabling Three-Party G.711 Ad Hoc Conferencing, page 117 • Defining XML API Schema, page 119

Table 1 Cisco Unified SRST Configuration Sequence (continued)

Chapter or Appendix	Description
Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource	Describes how to configure Cisco Unified Communications Manager and Cisco Unified SRST to enable multicast music-on-hold (MOH). This chapter includes the following tasks: • Configuring Cisco Unified Communications Manager for Cisco Unified SRST Multicast MOH, page 127 • Configuring Cisco Unified SRST for Multicast MOH, page 137 • Configuring Cisco Unified SRST MOH Live-Feed Support (Optional), page 145
Setting Up Secure SRST	Describes the Media and Signaling Authentication and Encryption feature for Cisco IOS MGCP gateways in SRST mode. This chapter includes the following tasks: • Preparing the Cisco Unified SRST Router for Secure Communication, page 161 • Importing Phone Certificate Files in PEM Format to the Secure SRST Router, page 170 • Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router, page 177 • Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 180 • Verifying Phone Status and Registrations, page 182
Integrating Voice Mail with Cisco Unified SRST	Describes how to set up voice mail. This chapter includes the following tasks: • Configuring Direct Access to Voice Mail, page 195 • Configuring Message Buttons, page 198 • Redirecting to Cisco Unified Communications Manager Gateway, page 200 • Configuring Call Forwarding to Voice Mail, page 200
Monitoring and Maintaining Cisco Unified SRST	Provides a list of useful **show** commands for monitoring and maintaining Cisco Unified SRST.
Enhanced 911 Services	Describes the new Enhanced 911 Services feature.
Appendix A: Preparing Cisco Unified SRST Support for SIP	Describes special configurations to support SIP calls.

Feature Roadmap

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

Table 2 Features by Cisco Unified SRST Software Version

Cisco Unified SRST	Enhancements or Modifications
Version 7.0/4.3	• Configuring Eight Lines Per Button (Octo-Line), page 75 • Configuring Consultative Transfer, page 86
Version 4.2(1)	Enhanced 911 Services, page 227 includes these new features: • Assigning ERLs to zones to enable routing to the PSAP that is closest to the caller • 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 • Expanding the E911 location information to include name and address • Adding new permanent call detail records
Version 4.1	Enhanced 911 Services, page 227
Version 4.0	• Additional Cisco Unified IP Phone Support, page 17 for the Cisco Unified IP Phone 7960G, 7911G, 7941G-GE, 7961G-GE • Cisco IP Communicator Support, page 17 • Fax Passthrough using SCCP and ATAs Support, page 17 • H.323 VoIP Call Preservation Enhancements for WAN Link Failures, page 18 • Video Support, page 18
Version 3.4	• Cisco SIP SRST 3.4, page 18
Version 3.3	• Secure SRST, page 19. • Cisco Unified IP Phone 7970G and Cisco Unified 7971G-GE Support, page 19 • Enhancement to the show ephone Command, page 19
Version 3.2	• Enhancement to the alias Command, page 20 • Enhancement to the pickup Command, page 20 • Enhancement to the user-locale Command, page 21 • Enhancement to the user-locale Command, page 21 • Increased the Number of Cisco Unified IP Phones Supported on the Cisco 3845, page 21 • MOH Live-Feed Support, page 21 • No Timeout for Call Preservation, page 21 • RFC 2833 DTMF Relay Support, page 21 • Translation Profile Support, page 22

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

Cisco Unified SRST	Enhancements or Modifications
Version 3.1	• Cisco Unified IP Phone 7920 Support, page 22 • Cisco Unified IP Phone 7936 Support, page 22
Version 3.0	—
	• Additional Language Options for IP Phone Display, page 23 • Consultative Call Transfer and Forward Using H.450.2 and H.450.3, page 23 • Customized System Message for Cisco Unified IP Phones, page 24 • Dual-Line Mode, page 24 • E1 R2 Signaling Support, page 24 • European Date Formats, page 25 • Huntstop for Dual-Line Mode, page 26 • Music on Hold for Multicast from Flash Files, page 26 • Ringing Timeout Default, page 26 • Secondary Dial Tone, page 26 • Enhancement to the show ephone Command, page 26 • System Log Messages for Phone Registrations, page 26 • Three-Party G.711 Ad Hoc Conferencing, page 27 • Support for Cisco VG248 Analog Phone Gateway Version 1.2(1) and Higher Versions, page 27
Version 2.1	• Cisco Unified IP Phone 7902G Support, page 28 • Cisco Unified IP Phone 7912G Support, page 29
	—
	• Additional Language Options for IP Phone Display, page 27 • Cisco SRST Aggregation, page 28 • Cisco ATA 186 and ATA 188 Support, page 28 • Cisco Unified IP Phone 7905G Support, page 28 • Cisco Unified IP Phone Expansion Module 7914 Support, page 29 • Enhancement to the dialplan-pattern Command, page 29
Version 2.02	• Cisco Unified IP Phone Conference Station 7935 Support, page 29. • Increase in Directory Numbers, page 30. • Cisco Unity Voice Mail Integration Using In-Band DTMF Signaling Across the PSTN and BRI/PRI, page 30. • Cisco Unified SRST was implemented on the Cisco Catalyst 4500 access gateway module and Cisco 7200 routers (NPE-225, NPE-300, and NPE400). • Support was removed for the Cisco MC3810-V3 concentrator.

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

Cisco Unified SRST	Enhancements or Modifications
Version 2.01	• Cisco Unified SRST was implemented on the Cisco 1760 routers, and support for the Cisco 1750 was removed. • Support was added for additional connected Cisco IP phones. • Support was added for additional directory numbers or virtual voice ports on Cisco IP phones.
Version 2.0	Cisco Unified SRST was implemented on the Cisco 2600XM and Cisco 2691 routers.
	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.
	• Cisco Unified SRST was implemented on the Cisco 1750 and Cisco 1751 routers. • Huntstop support. • Class of restriction (COR). • Translation rule support. • Music on hold and tone on hold. • Distinctive ringing. • Forward to a central voice mail or auto-attendant (AA) through PSTN during Cisco Unified Communications Manager fallback. • Phone number alias support during Cisco Unified Communications Manager fallback: enhanced default destination support. • List-based call restrictions for Cisco Unified Communications Manager fallback.

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

Cisco Unified SRST	Enhancements or Modifications
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 reestablished. • 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.

Information About New Features in Cisco Unified SRST

This section contains the following topics:

New Features in Cisco Unified SRST V4.3/7.0

Cisco Unified SRST 7.0/4.3 supports the following new features:

- Configuring Eight Lines Per Button (Octo-Line), page 75
- Configuring Consultative Transfer, page 86

New Features in Cisco Unified SRST V4.2(1)

Cisco Unified SRST Version 4.2(1) indroduces the following new features:

- Enhancements for Enhanced 911 Services, page 227

New features in Cisco Unified SRST V4.1

Cisco Unified SRST Version 4.1 introduces the following new feature:

- Enhanced 911 Services, page 227

New Features in Cisco Unified SRST V4.0

Cisco Unified SRST Version 4.0 has introduced the following new features:

- Additional Cisco Unified IP Phone Support, page 17
- Cisco IP Communicator Support, page 17
- Fax Passthrough using SCCP and ATAs Support, page 17
- H.323 VoIP Call Preservation Enhancements for WAN Link Failures, page 18
- Video Support, page 18

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 the *Cisco IP Phone 7914 Expansion Module Quick Start Guide* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7916/english/16enug.pdf

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 the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html

To determine compatible firmware, platforms, memory, and additional voice products that are associated with Cisco Unified SRST 4.0, see the following documentation:

Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products at the following URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html

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 Passthrough using SCCP and ATAs Support

Fax passthrough 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 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 the Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP, at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cata/186_188/2_15_ms/english/administration/guide/sccp/sccpach5.html.

H.323 VoIP Call Preservation Enhancements for WAN Link Failures

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.

For configuration information see the “Configuring H.323 Gateways” chapter in the *Cisco IOS H.323 Configuration Guide*, Release 12.4T.

Video Support

This feature allows you to set video parameters for the Cisco Unified SRST to maintain close feature parity with Cisco Unified Communications Manager. 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 Communications Manager. 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 211.

New Features in Cisco SRST V3.4

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

- Cisco SIP SRST 3.4

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 proxy server 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 the *Cisco SIP SRST Version 3.4 System Administrator Guide*.

New Features in Cisco SRST V3.3

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

- Secure SRST, page 19
- Cisco Unified IP Phone 7970G and Cisco Unified 7971G-GE Support, page 19
- Enhancement to the show ephone Command, page 19

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 "Setting Up Secure SRST" section on page 153.

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 customizeable 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 29 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 the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

New Features in Cisco SRST V3.2

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

- Enhancement to the alias Command, page 20
- Enhancement to the cor Command, page 20
- Enhancement to the pickup Command, page 20
- Enhancement to the user-locale Command, page 21
- Increased the Number of Cisco Unified IP Phones Supported on the Cisco 3845, page 21
- MOH Live-Feed Support, page 21
- No Timeout for Call Preservation, page 21
- RFC 2833 DTMF Relay Support, page 21
- Translation Profile Support, page 22

Enhancement to the alias Command

The **alias** command is enhanced as follows:

- The **cfw** keyword was added, providing call forward no-answer/busy capabilities.
- 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 the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

Enhancement to the cor Command

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

For more information, see the **cor** command in the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

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 the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

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)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

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. For more information, see *Cisco IOS Survivable Remote Site Telephony (SRST) 3.2 Specifications for Cisco IOS Software Release 12.3(11)T.*

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 adapter 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 121 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 Description" section on page 33 for more information.

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 Appendix A: Preparing Cisco Unified SRST Support for SIP, page 265 for configuration instructions.

To use voice mail 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 92 for more configuration information. For more information on the **translation-profile**, command see the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

New Features in Cisco SRST V3.1

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

- Cisco Unified IP Phone 7920 Support, page 22
- Cisco Unified IP Phone 7936 Support, page 22

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 Communications Manager 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 V3.0

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

- Additional Language Options for IP Phone Display, page 23
- Consultative Call Transfer and Forward Using H.450.2 and H.450.3, page 23
- Customized System Message for Cisco Unified IP Phones, page 24
- Dual-Line Mode, page 24
- E1 R2 Signaling Support, page 24
- European Date Formats, page 25
- Huntstop for Dual-Line Mode, page 26
- Music on Hold for Multicast from Flash Files, page 26
- Ringing Timeout Default, page 26
- Secondary Dial Tone, page 26
- Enhancement to the show ephone Command, page 26
- System Log Messages for Phone Registrations, page 26
- Three-Party G.711 Ad Hoc Conferencing, page 27
- Support for Cisco VG248 Analog Phone Gateway Version 1.2(1) and Higher Versions, page 27

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.

Note This feature is available only for Cisco SRST running under Cisco Unified Communications Manager V3.2.

Consultative Call Transfer and Forward Using H.450.2 and H.450.3

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 PSTN interface type.

For consultative transfer to be available, the Cisco SRST router must be configured with the dual-line mode. See the “Configuring Dual-Line Phones” section on page 72.

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.

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 100.

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 70.

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 72.

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 68.

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 96.

Music on Hold for Multicast from Flash Files

Cisco 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 119.

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 98.

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 72.

Enhancement to the show ephone Command

The **show ephone** command is enhanced to display the following:

- The configuration and status of additional phones (new keywords: **7905**, **7914**, **7935**, **ATA**)
- The 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 the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

System Log Messages for Phone Registrations

Diagnostic messages are added to the system log whenever a phone registers or unregisters from Cisco 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 117.

Support for Cisco VG248 Analog Phone Gateway Version 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 Communications Manager.

During Cisco Unified Communications Manager 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 the *Cisco VG248 Analog Phone Gateway Data Sheet* and the *Cisco VG248 Analog Phone Gateway Version 1.2(1) Release Notes*.

New Features in Cisco SRST V2.1

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

- Additional Language Options for IP Phone Display, page 27
- Cisco SRST Aggregation, page 28
- Cisco ATA 186 and ATA 188 Support, page 28
- Cisco Unified IP Phone 7902G Support, page 28
- Cisco Unified IP Phone 7905G Support, page 28
- Cisco Unified IP Phone 7912G Support, page 29
- Cisco Unified IP Phone Expansion Module 7914 Support, page 29
- Enhancement to the dialplan-pattern Command, page 29

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 SRST running under Cisco Unified Communications Manager V3.2.

For configuration information, see the "Configuring IP Phone Language Display" section on page 69.

Cisco SRST Aggregation

For systems running Cisco Unified Communications Manager 3.3(2) and later, 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 in order 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 the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html.

New Features in Cisco SRST V2.02

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

- Cisco Unified IP Phone Conference Station 7935 Support, page 29
- Increase in Directory Numbers, page 30
- Cisco Unity Voice Mail Integration Using In-Band DTMF Signaling Across the PSTN and BRI/PRI, page 30

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 7935 dynamically registers to Cisco Unified Communications Manager for connection services and receives the appropriate endpoint phone number and any software enhancements or personalized settings, which are preloaded within Cisco Unified Communications Manager.

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

Directory numbers were increased for the routers shown in Table 3.

Table 3 Increases in Directory Numbers in Cisco IOS Release 12.2(11)T

		Increase in Maximum Directory Number	
Cisco Router	**Maximum Phones**	**From**	**To**
Cisco 1751	24	96	120
Cisco 1760	24	96	120
Cisco 2600XM	24	96	120
Cisco 2691	72	216	288
Cisco 3640	72	216	288
Cisco 3660	240	720	960
Cisco 3725	144	432	576
Cisco 3745	240	720	960

Cisco Unity Voice Mail Integration Using In-Band DTMF Signaling Across the PSTN and BRI/PRI

Cisco Unity Voice Mail and other voice-mail systems can be integrated with Cisco SRST. Voice-mail 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

For further command information, see the *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* and the “Integrating Voice Mail with Cisco Unified SRST” section on page 193.

For information about monitoring and maintaining Cisco Unified SRST, go to the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Proceed to the “Overview of Cisco Unified SRST” section on page 33.

Overview of Cisco Unified SRST

Revised: July 11, 2008

This chapter describes Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) and what it does. It also includes information about Cisco Unified IP Phone, platform, and Cisco Unified Communications Manager version support, specifications, features, restrictions, and where to find additional reference documents.

Note For the most up-to-date information about Cisco Unified IP Phone support, the maximum number of Cisco Unified IP Phones, maximum DNs or virtual voice ports, and memory requirements for Cisco Unified SRST, see the *Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html.

Contents

Cisco Unified SRST Description

Cisco Unified SRST provides Cisco Unified Communications Manager with fallback support for Cisco 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 IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Unified Communications Manager installations or when the WAN connection is down.

Cisco Unified Communications Manager supports Cisco IP phones at remote sites attached to Cisco multiservice routers across the WAN. Prior to Cisco Unified SRST, when the WAN connection between a router and the Cisco Unified Communications Manager failed or when connectivity with Cisco Unified Cisco Unified Communications Manager 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 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 IP phones that are registered with the router. When the WAN link or connection to the primary Cisco Unified Communications Manager is restored, call handling reverts back to the primary Cisco Unified Communications Manager.

When Cisco Unified IP Phones lose contact with primary, secondary, and tertiary Cisco Unified Communications Managers, 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 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 Communications Manager accommodates a maximum of three entries. When a secondary Cisco Unified Communications Manager is not available on the network, the local Cisco Unified SRST Router's IP address is retained as the standby connection for Cisco Unified Communications Manager during normal operation.

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

Typically, it takes three times the keepalive period for a phone to discover that its connection to Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager in its Unified Communications Manager list. Otherwise, the phone activates a standby connection to its secondary Cisco Unified Communications Manager.

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 Communications Managers in its Cisco Unified Communications Manager list, it progresses through its list of secondary and tertiary Cisco Unified Communications Managers before attempting to connect with its local Cisco Unified SRST router. Therefore, the time that passes before the Cisco IP Phone eventually establishes a connection with the Cisco Unified SRST router increases with each attempt to contact to a Cisco Unified Communications Manager. Assuming that each attempt to connect to a Cisco Unified Communications Manager takes about one minute, the Cisco IP phone in question could remain offline for three 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 Communications Manager fallback mode. 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 Communications Manager fallback mode. When the Cisco Unified Communications Manager is restored, the message goes away and full Cisco Unified IP Phone functionality is restored.

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

Once a connection is reestablished with Cisco Unified Communications Manager, 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 Communications Manager and Cisco Unified SRST. A Cisco Unified IP phone cannot reestablish a connection with the primary Cisco Unified Communications Manager at the central office if it is currently engaged in an active call.

Figure 1 shows a branch office with several Cisco IP phones connected to a Cisco Unified SRST router. The router provides connections to both a WAN link and the PSTN. The Cisco Unified IP phones connect to their primary Cisco Unified Communications Manager at the central office via this WAN link.

Figure 1 Branch Office Cisco Unified IP Phones Connected to a Remote Central Cisco Unified Communications Manage

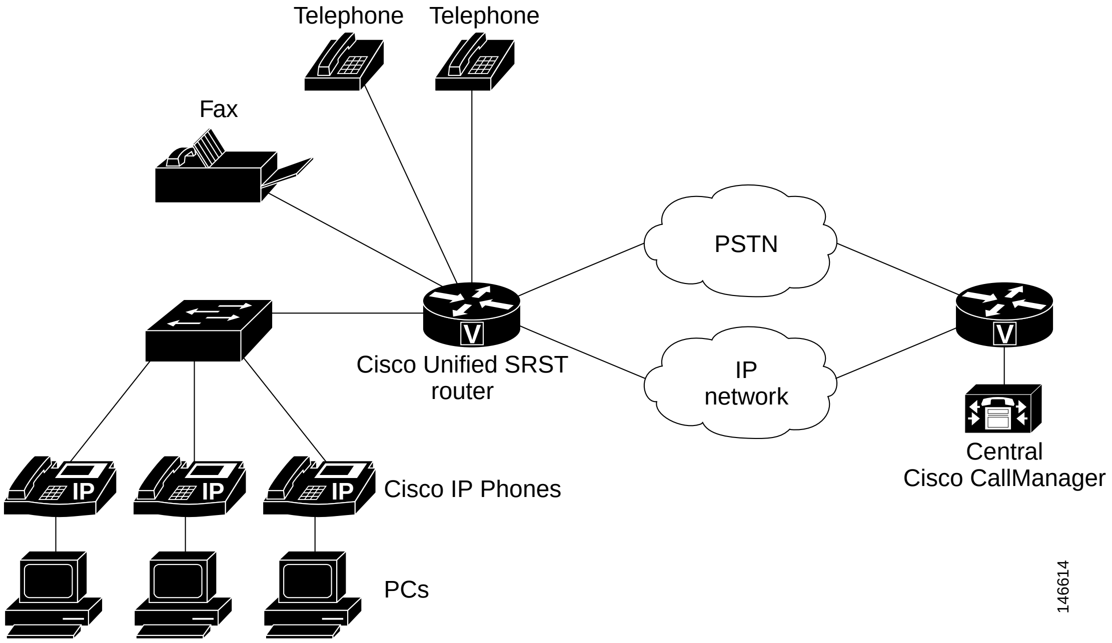
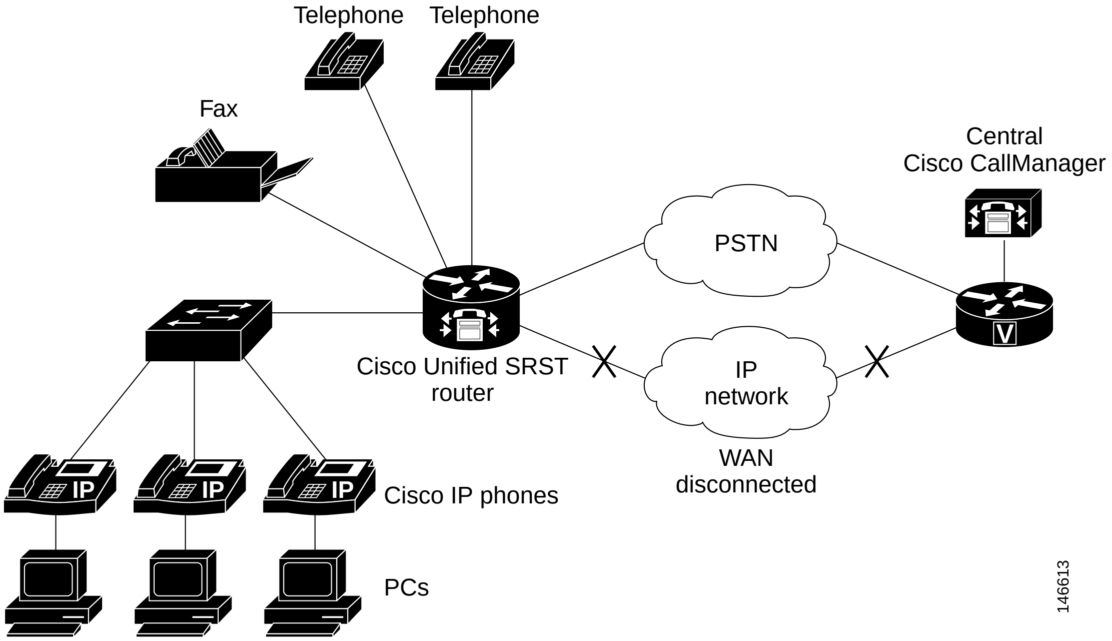


Figure 2 shows the same branch office telephone network with the WAN connection down. In this situation, the Cisco IP phones use the Cisco Unified SRST router as a fallback for their primary Cisco Unified Communications Manager. The branch office Cisco Unified IP Phones are connected to the PSTN through the Cisco Unified SRST router and are able to make and receive off-net calls.

Figure 2 Branch Office Cisco Unified IP Phones Connected to a Remote Central Cisco Unified Communications Manage Operating in SRST Mode



On H.323 gateways, 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.

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 “Enabling SRST on an MGCP Gateway” section on page 52.

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.

Support for Cisco Unified IP Phones, Platforms, Cisco Unified Communications Manager, Signals, Languages, and Switches

The following sections provide information about Cisco Feature Navigator and the histories of Cisco Unified IP Phone, platform, and Cisco Unified Communications Manager 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 38
- Cisco Unified IP Phone Support, page 38
- Platform and Memory Support, page 39
- Cisco Unified Communications Manager Compatibility, page 40
- Signal Support, page 40
- Language Support, page 40

- Switch Support, page 40

Finding Cisco IOS Software Releases That Support Cisco Unified SRST

The tables in this chapter list only the Cisco IOS software releases that first introduce new features to Cisco Unified SRST. Other Cisco IOS software releases may subsequently inherit versions of Cisco Unified SRST. To get a list of Cisco IOS software releases that support a particular version of Cisco Unified SRST, use Cisco Feature Navigator.

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 the *Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html.

The following IP phones are supported by Cisco Unified SRST 4.0:

- Cisco Analog Telephone Adaptor (ATA) 186 and Cisco ATA 188 Version 2.16 and later versions with Cisco Unified Communications Manager 3.3 and later versions

  Cisco Unified SRST supports Cisco ATA 186 and Cisco ATA 188 using Skinny Client Control Protocol (SCCP) for voice calls only

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 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 the Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP, at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cata/186_188/2_15_ms/english/administration/guide/sccp/sccpach5.html .

- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7910
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G
- Cisco Unified IP Phone Expansion Module 7914
- Cisco Unified Wireless IP Phone 7920
- Cisco IP Conference Station 7935
- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Phone 7940G
- Cisco Unified IP Phone 7941G, Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7960G

- Cisco Unified IP Phone 7961G, Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco VG224 Analog Phone Gateway, IOS Version 12.4(4)XC with Cisco Unified SRST 4.0 running Cisco IOS Software Release 12.4(4)XC and later. For configuration information see, the "Enabling Fallback to Cisco Unified SRST on the Voice Gateway" section in *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways* at the following URL: http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ht1vg224.html.
- Cisco VG248 Analog Phone Gateway Version 1.2(1) and higher versions.

Note During Cisco Unified Communications Manager 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 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 the *Cisco VG248 Analog Phone Gateway Data Sheet* and the *Cisco VG248 Analog Phone Gateway Version 1.2(1) Release Notes*.

Platform and Memory Support

For the most up-to-date information about the maximum number of Cisco Unified IP Phones, maximum DNs or virtual voice ports, and memory requirements for Cisco Unified SRST, see the *Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html.

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.

Note For the most up-to-date information about Cisco IOS software images, see the *Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html.

Cisco Unified Communications Manager Compatibility

See the Cisco Unified Communications Manager Compatibility Matrix.

Signal Support

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

Language Support

Cisco SRST 3.2 and later supports the following languages:

- Danish
- Dutch
- English
- French
- German
- Italian
- Japanese Katakana (available under Cisco Unified Communications Manager 4.0 or later).
- Norwegian
- Portuguese
- Russian
- Spanish
- Swedish

Note The Cisco Unified IP Phone 7911G, Cisco Unified IP Phone 7941G and 7941G-GE, Cisco Unified IP Phone 7961G and 7961G-GE, Cisco Unified IP Phone 7970G, and Cisco Unified IP Phone 7971G-GE support English only.

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)

Prerequisites for Configuring Cisco Unified SRST

Before configuring Cisco Unified SRST you must do the following:

- You have an account on Cisco.com to download software.

  To obtain an account on Cisco.com, go to www.cisco.com and click **Register** at the top of the screen.
- You have purchased a Cisco Unified SRST license.

  To purchase a license, go to http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key.
- Choose an appropriate Cisco Unified SRST version. Each SRST version supports a specific set of IP phones, memory requirements, features, and directory numbers (DNs). See the "Platform and Memory Support" section on page 39 and the "Restrictions for Configuring Cisco Unified SRST" section on page 43.
- Choose an appropriate phoneload. SRST only supports certain phoneloads that have been tested with the various Cisco Unified Communications Manager versions. For the most up-to-date phoneloads, see the *Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html.
- If you have Cisco Unified Communications Manager already installed, verify that your version of Cisco Unified Communications Manager is compatible with your Cisco Unified SRST release. See the "Cisco Unified Communications Manager Compatibility" section on page 40.

Prerequisites for Version

- For general prerequisites, see the "Prerequisites for Configuring Cisco Unified SRST" section on page 41.
- For the prerequisites for Enhanced 911 Services, see the "Prerequisites" section on page 227.

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 (CallManager) Install and Upgrade Guides at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

- Integrate Cisco Unified SRST with Cisco Unified Communications Manager. Integration is performed from Cisco Unified Communications Manager. See the“Integrating Cisco Unified SRST with Cisco Unified Communications Manager” section on page 42.

Installing Cisco Unified SRST

Cisco Unified SRST versions have different installation instructions:

- Installing Cisco SRST V3.0 and Later Versions, page 42
- Installing Cisco SRST V2.0 and V2.1, page 42
- Installing Cisco SRST V1.0, page 42

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

Installing Cisco 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 40. Cisco IOS software can be downloaded from the Cisco Software Center at 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 119. If you plan use music on hold, go to the Technical Support Software Download site at 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 SRST V2.0 and V2.1

Download and install Cisco SRST V2.0 or Cisco SRST V2.1 from the Cisco Software Center at http://www.cisco.com/public/sw-center/.

Installing Cisco 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 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 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 SRST

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

Table 1 History of Restrictions from Cisco SRST V1.0 to the Present Cisco Unified SRST Version

Cisco SRST Version	Cisco IOS Release	Restrictions
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 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 the “Precautions for Mobile Phones” section on page 233. • The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL). For more information, see the “Overview” section on page 228. • 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” section on page 236. • 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 Service _and existing Cisco Unified SRST features, see the “Interactions with Existing Cisco Unified SRST Features” section on page 236.

Table 1 History of Restrictions from Cisco SRST V1.0 to the Present Cisco Unified SRST Version (continued)

Cisco SRST Version	Cisco IOS Release	Restrictions
Version 4.0	12.4(4)XC	• All of the restrictions in Cisco SRST Version 1.0. • Call transfer is supported only on the following: – 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 – FXO and FXS loop-start (analog) – FXO and FXS ground-start (analog) – Ear and mouth (E&M) (analog) and DID (analog) – T1 channel-associated signaling (CAS) with FXO and FXS ground-start signaling – T1 CAS with E&M signaling – All PRI and BRI switch types • The following Cisco Unified IP Phone function keys are dimmed because they are not supported during SRST operation: – MeetMe – GPickUp (group pickup) – Park – Confrn (conference) • 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.
Version 3.4	12.4(4)T	
Version 3.3	12.3(14)T	
Version 3.2	12.3(11)T	
Version 3.1	12.3(7)T	
Version 3.0	12.2(15)ZJ	
Version 2.1	12.2(15)T	
Version 2.02	12.2(13)T	
Version 2.01	12.2(11)T	
Version 2.0	12.2(8)T1	
Version 2.0	12.2(8)T	
Version 2.0	12.2(2)XT	
Version 1.0	12.2(2)XB	• Does not support first generation Cisco Unified IP Phones, such as Cisco IP Phone 30 VIP and Cisco IP Phone 12 SP+. • Does not support other Cisco Unified Communications Manager applications or services: Cisco IP SoftPhone, Cisco uOne: Voice and Unified Messaging Application, or Cisco IP Contact Center. • Does not support Centralized Automatic Message Accounting (CAMA) trunks on the Cisco 3660 routers. **Note** 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.
	12.2(2)XG	
	12.1(5)YD	

Where to Go Next

The next chapters of this guide describe how to configure Cisco Unified SRST. As shown in Table 2, each chapter takes you through these 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 is configured correctly for Cisco Unified SRST. For instructions, see the "Prerequisites for Configuring Cisco Unified SRST" section on page 41.

Table 2 Cisco Unified SRST Configuration Sequence

Task	Where Task Is Described
1. Setting up a Cisco Unified SRST system to communicate with your network	"Setting Up the Network" chapter
2. Setting up the basic Cisco Unified SRST phone configuration	"Setting Up Cisco Unified IP Phones" chapter
3. Configuring incoming and outgoing calls	"Setting Up Call Handling" chapter
4. Configuring optional system and phone parameters	"Configuring Additional Call Features" chapter
5. Configuring optional security for SRST	"Setting Up Secure SRST" chapter
6. Setting up voice mail	"Integrating Voice Mail with Cisco Unified SRST" chapter
7. Configuring Enhanced 911 Services	"Enhanced 911 Services" chapter

Additional References

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

- Related Documents, page 46
- Standards, page 48
- MIBs, page 48
- RFCs, page 48
- Technical Assistance, page 48

Related Documents

Related Topic	Documents
Cisco IOS voice 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 IP phones	*Cisco IP Phones and Services*
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*

Related Topic	Documents
Cisco SRST command reference	*Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference*
Cisco Unified Communications Manager music on hold	The "Music On Hold" chapter of the *Cisco Unified CallManager and Cisco Unified IP Phone Administrator's A - Z Feature Guide* for your specific Cisco Unified Communications Manager release. From the Cisco Unified Communications Manager documentation directory, click **Cisco Unified Communications Manager (CallManager)** > **Maintain and Operate Guides**.
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 IP Phone 7970 Administration Guide for Cisco Communications Manager, Release 4.x and later, "Understanding Security Features for Cisco IP Phones" section.*
Cisco Unified SRST commands and specifications	• *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)* • *Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products*
Command reference and configuration information for voice and SRST	• *Cisco IOS Voice Command Reference* • *Cisco IOS Debug Command Reference* • *Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide* • *Cisco SRST 3.2 Command Reference*
Command reference and configuration information for voice and telephony commands	• *Cisco IOS Voice Command Reference* • *Cisco IOS Debug Command Reference*
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
DHCP	• *Cisco IOS DHCP Server*
Media Inactive Call Detection	• *Media Inactive Call Detection*
Phone documentation for Cisco Unified SRST	• *Cisco Unified IP Phones 7900 Series* • *Survivable Remote Site Telephony*
Standard Glossary	• *Cisco IOS Voice Configuration Library Glossary*
Standard Preface	• *Cisco IOS Voice Configuration Library Preface*

Standards

Standard	Title
ITU X. 509 Version 3	*Public-Key and Attribute Certificate Frameworks*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2246	*The Transport Layer Security (TLS) Protocol Version 1.0*
RFC 3711	*The Secure Real-Time Transport Protocol (SRTP)*

Technical Assistance

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

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

Setting Up the Network

Revised: July 11, 2008

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

When the WAN link fails, the Cisco Unified IP Phones detect that they are no longer receiving keepalive packets from Cisco Unified Communications Manager. 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 Communications Manager 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 52 (Required)
- Enabling SRST on an MGCP Gateway (Required)
- Configuring DHCP for Cisco Unified SRST Phones, page 58 (Required)
- Specifying Keepalive Intervals, page 61 (Optional)
- Configuring Cisco Unified SRST to Support Phone Functions, page 62 (Required)
- Verifying That Cisco Unified SRST Is Enabled, page 64 (Optional)

Enabling IP Routing

For information about enabling IP routing, see *Configuring IP Addressing*.

Enabling 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.

Note 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.

Note 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 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
   service [**alternate** | **default**] *service-name location*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password when prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ccm-manager fallback-mgcp`**
	Example:
	`Router(config)# ccm-manager fallback-mgcp`
		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.

	Command or Action	Purpose

Step 4	**`call application alternate`** `[`*`application-name`*`]`
	`or`
	`service` `[`**`alternate`** `|` **`default`**`]` *`service-name location`*
	Example:
	`Router(config)# call application alternate`
	`or`
	`Router(config)# service default`
		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.
		Or
		The **service** command loads and configures a specific, standalone application on a dial peer. The keywords and arguments are as follows:
		• **alternate** (Optional). Alternate service to use if the service that is configured on the dial peer fails.
		• **default** (Optional). Specifies that the default service ("DEFAULT") on the dial peer is used if the alternate service fails.
		• *service-name*: Name that identifies the voice application.
		• *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

Step 5	**`exit`**
	Example:
	`Router(config)# exit`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring SRST on an MGCP Gateway Using Cisco IOS Release 12.3(14)T or Later

Perform this task to enable SRST on a 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.

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

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password when prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ccm-manager fallback-mgcp`**
	Example:
	`Router(config)# ccm-manager fallback-mgcp`
		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.

Step 4	**`application`** `[`*`application-name`*`]`
	Example:
	`Router(config) application app-xfer`
		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	**`global`**
	Example:
	`Router(config)# global`
		Enters Global configuration mode.

	Command or Action	Purpose
Step 6	**service** [*alternate* | *default*] *service-name location* **Example:** `Router(config) service myapp https://myserver/myfile.vxml`	Loads and configures a specific, standalone application on a dial peer. • **alternate** (Optional). Alternate service to use if the service that is configured on the dial peer fails. • **default** (Optional). Specifies that the default service ("DEFAULT") on the dial peer is used if the alternate service fails. • *service-name*: Name that identifies the voice application. • *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.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

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 a MGCP Gateway if you are using Cisco IOS Release 12.3(14)T or later version.

```
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-l3 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
mgcp dtmf-relay voip codec all mode cisco
mgcp package-capability rtp-package
mgcp sdp 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 refer to 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 UnifiedIP Phones:

- Defining a Single DHCP IP Address Pool, page 58: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 59: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 60: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 some (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

	Command or Action	Purpose
Step 8	`ip dhcp pool` *pool-name* **Example:** `Router(config)# ip dhcp pool mypool`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 9	`network` *ip-address* [*mask* | *prefix-length*] **Example:** `Router(config-dhcp)# network 10.0.0.0 255.255.0.0`	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.
Step 10	`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 Communications Manager.
Step 11	`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 12	`exit`
	Example:
	`Router(config-dhcp)# exit`
		Exits DHCP pool configuration mode.

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-mas*k
3. **option 150 ip** *ip-address*
4. **default-router** *ip-address*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool pool2`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
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 Communications Manager.
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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`service dhcp`**
	Example:
	`Router(config)# service dhcp`
		Enables the Cisco IOS DHCP Server feature on the router.

Step 2	**`interface`** *`type number`*
	Example:
	`Router(config)# interface serial 0`
		Enters interface configuration mode for the specified interface. See the *Cisco IOS Interface and Hardware Component Command Reference, Release 12.3T* for more information.

Step 3	**`ip helper-address`** *`ip-address`*
	Example:
	`Router(config-if)# ip helper-address 10.0.22.1`
		Specifies the helper address for any unrecognized broadcast for TFTP server and Domain Name System (DNS) requests. For each server, a separate **ip helper-address** command is required if the servers are on different hosts. You can also configure multiple TFTP server targets by using the **ip helper-address** commands for multiple servers.

Step 4	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode.

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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`keepalive`** *`seconds`*
	Example:
	`Router(config-cm-fallback)# keepalive 60`
		Sets the time interval, in seconds, between keepalive messages that are sent to the router by Cisco Unified IP Phones.
		• *seconds*:Range is 10 to 65535. Default is 30.

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

Example

The following example sets a keepalive interval of 45 seconds:

```
call-manager-fallback
 keepalive 45
```

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** {**7910** | **7935** | **7940** | **7960**} *max-lines*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-manager-fallback** **Example:** `Router(config)# call-manager-fallback`	Enters call-manager-fallback configuration mode.
Step 2	**ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**] **Example:** `Router(config-cm-fallback)# ip source-address 10.6.21.4 port 2002 strict-match`	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.
Step 3	**max-dn** *max-directory-numbers* [**dual-line**] [**preference** *preference-order*] **Example:** `Router(config-cm-fallback)# max-dn 15 dual-line preference 1`	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. • *max-directory-numbers:* 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 39 for further details. • **dual-line** (Optional). Allows IP phones in Cisco Unified Communications Manager fallback mode to have a virtual voice port with two channels. • **preference** *preference-order* (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 **alias** command also has a **preference** keyword that sets **alias** command preference values. Setting the **alias** command **preference** keyword allows the default preference set with the **max-dn** command to be overridden. See Configuring Call Rerouting, page 81 for more information on using the **max-dn** command with the **alias** command. **Note** You must reboot the router in order to reduce the limit of the directory numbers or virtual voice ports after the maximum allowable number is configured.

	Command or Action	Purpose

Step 4	**`max-ephones`** *`max-phones`*
	Example:
	`Router(config-cm-fallback)# max-ephones 24`
		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 the "Platform and Memory Support" section on page 39 for further details.
		Note You must reboot the router in order to reduce the limit of Cisco IP phones after the maximum allowable number is configured.

Step 5	**`limit-dn`** `{`**`7910`** `|` **`7935`** `|` **`7940`** `|` **`7960`**`}` *`max-lines`*
	Example:
	`Router(config-cm-fallback)# limit-dn 7910 2`
		Limits the directory number lines on Cisco IP phones during Cisco Unified Communications Manager fallback.
		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.
		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`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 in order 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. Enter the **no** form of the appropriate **access-list** command to restore normal service for the phone.

c. Use the **debug ephone register** command to observe the registration process of the Cisco IP phone on the Cisco Unified SRST router.

d. Use the **show ephone** command to display the Cisco IP phones that have registered to the Cisco Unified SRST router.

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 the *Cisco IOS Debug Command Reference* for your Cisco IOS Software Release by going to Cisco IOS Software Support Resources and clicking the appropriate release version and **Command References**.

Where to Go Next

The next step is setting up the phone and getting a dial tone. For instructions, see the "Setting Up Cisco Unified IP Phones" chapter.

For additional information, see the "Additional References" section on page 46 in the Overview of Cisco Unified SRST chapter.

Setting Up Cisco Unified IP Phones

Revised: July 11, 2008

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 Communications Manager fallback.

Contents

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 Communications Manager settings during Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager fallback.

How to Set Up Cisco Unified IP Phones

This section contains the following tasks:

- Configuring IP Phone Clock, Date, and Time Formats, page 68 (Optional)
- Configuring IP Phone Language Display, page 69 (Optional)
- Configuring Customized System Messages for Cisco Unified IP Phones, page 70 (Optional)
- Configuring a Secondary Dial Tone, page 72 (Optional)
- Configuring Dual-Line Phones, page 72 (Required Under Certain Conditions)

- Configuring Eight Lines Per Button (Octo-Line), page 75 (Optional)

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 Phone7940, 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 Communications Manager 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

	Command or Action	Purpose
Step 1	**`clock timezone`** *`zone hours-offset`* [*`minutes-offset`*] **Example:** `Router(config)# clock timezone PST -8`	Sets the time zone for display purposes. • *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`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

	Command or Action	Purpose

Step 3	`date-format {mm-dd-yy | dd-mm-yy | yy-dd-mm | yy-mm-dd}`
	Example:
	`Router(config-cm-fallback)# date-format yy-dd-mm`
		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**.

Step 4	`time-format {12 | 24}`
	Example:
	`Router(config-cm-fallback)# time-format 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.

Step 5	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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
Rounter(config)# call-manager-fallback
Rounter(config-cm-fallback)# time-format 24
```

Configuring IP Phone Language Display

During Cisco Unified Communications Manager 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 Communications Manager V3.2 and later. Systems with software prior to Cisco Unified SRST V2.1 and Cisco Unified Communications Manager 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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`user-locale`** *`country-code`*
	Example:
	`Router(config-cm-fallback)# user-locale ES`
		Selects a language by country for displays on the Cisco IP Phone 7940 and Cisco IP Phone 7960.
		The following ISO-3166 codes are available to Cisco SRST and Cisco Unified SRST systems running under Cisco Communications Manager V3.2 or later versions:
		• **DE**:German.
		• **DK**:Danish.
		• **ES**:Spanish.
		• **FR**:French.
		• **IT**:Italian.
		• **JP**:Japanese Katakana (available under Cisco Unified Communications Manager V4.0 or later versions).
		• **NL**:Dutch.
		• **NO**:Norwegian.
		• **PT**:Portuguese.
		• **RU**:Russian.
		• **SE**:Swedish.
		• **US**:United States English (default).

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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

The **system message** command is used to customize the system message displayed on all Cisco Unified IP Phone 7910, Cisco Unified IP Phone 7940G, and Cisco Unified IP Phone 7960G units during Cisco Unified Communications Manager 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, such as the Cisco IP Phone 7940 and Cisco IP Phone 7960 units. 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, such as the Cisco IP Phone 7910. 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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`system message`** {**`primary`** *`primary-string`* | **`secondary`** *`secondary-string`*}
	Example:
	`Router(config-cm-fallback)# system message primary Custom Message`
		Declares the text for the system display message on IP phones in fallback mode.
		• **primary** *primary-string*: For Cisco Unified IP Phones that can support static text messages during fallback, such as the Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7960 units. A string of approximately 27 to 30 characters is allowed.
		• **secondary** *secondary-string*: For Cisco Unified IP Phones that do not support static text messages, such as the Cisco Unified IP Phone 7910. A string of approximately 20 characters is allowed.

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	`secondary-dialtone` *`digit-string`*
	Example:
	`Router(config-cm-fallback)# secondary-dialtone 9`
		Activates a secondary dial tone when a digit string is dialed.

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 Communications Manager fallback. Consultative transfer is also required (see the “Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0” section on page 100).

Dual-line IP phones are supported during Cisco Unified Communications Manager fallback using the **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 96.

SUMMARY STEPS

1. **call-manager-fallback**
2. **max-dn** *max-directory-numbers* [**dual-line**] [**preference** *preference-order*]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-manager-fallback** **Example:** Router(config)# call-manager-fallback	Enters call-manager-fallback configuration mode.
Step 2	**max-dn** *max-directory-numbers* [**dual-line**] [**preference** *preference-order*] **Example:** Router(config-cm-fallback)# max-dn 15 dual-line preference 1	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. • *max-directory-numbers:* 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 39 for further details. • **dual-line** (Optional). Allows IP phones in Cisco Unified Communications Manager fallback mode to have a virtual voice port with two channels. • **preference** *preference-order* (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 **alias** command also has a **preference** keyword that sets **alias** command preference values. Setting the **alias** command **preference** keyword allows the default preference set with the **max-dn** command to be overridden. See Configuring Call Rerouting, page 81 for more information on using the **max-dn** command with the **alias** command.
Step 3	**exit** **Example:** Router(config-cm-fallback)# exit	Exits call-manager-fallback configuration mode.

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 Communications Manager fallback mode.

```
call-manager-fallback
 max-dn 10 dual-line
 exit
```

Configuring Eight Lines 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 Communications Manager 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.
- The maximum number of directory numbers must be equal to or greater than the total of all line combinations.
- SIP endpoints are not supported on H.323 trunks. SIP endpoints are supported on SIP trunks only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**

4. **max-dn** *max-no-of-directories* [dual-line | octo-line] [<*num*> octo-line]
5. **huntstop channel** *1-8*
6. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 4	**`max-dn`** *`max-no-of-directories`* `[dual-line	octo-line] [<`*`num`*`> octo-line]` **Example:** `Router(config-cm-fallback)# max-dn 15 dual-line 6 octo-line`	Sets the maximum number of directory numbers (dn) or virtual voice ports that can be supported by the router and activates dual-line mode, octo-line mode, or both modes. • max-directory-numbers: Maximum number of directory numbers or virtual voice ports supported by the router. The maximum number is platform-dependent. The default is 0. • dual-line: (Optional) Allows IP phones in Cisco Unified Communications Manager fallback mode to have a virtual voice port with two channels. • octo-line: (Optional) Allows IP phones in Cisco Unified Communications Manager fallback mode to have a virtual voice port with eight channels. • num (Optional): Sets the number of directory numbers for octo-mode. The range is 0-8 and the default is 8.

Step 5	**`huntstop channel`** *`1-8`*
	Example:
	`Router(config-cm-fallback)# huntstop channel 4`
		Enables channel huntstop on an octo-line, which keeps a call from hunting to the next channel of a directory number if the last allowed channel is busy or does not answer.
		• *number*: Number of channels available to accept incoming calls. The remaining channels are reserved for outgoing calls and features such as call transfer, call waiting, and conferencing. The range is 1-8 and the default is 8.
		• The command is supported for octo-line directory numbers only.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

Example

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
!
```

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 key pad, 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 SRST TFTP server
- Headset with microphone for your PC (Optional; you can use PC internal speakers and microphone)

SUMMARY STEPS

1. Download the latest version of the Cisco IP Communicator software and install it on your PC.
2. (Optional) Attach the headset to your PC.
3. Start the Cisco IP Communicator software application.
4. Define the IP address of the Cisco Unified SRST TFTP server.
5. Wait for the Cisco IP Communicator application to connect to the Cisco Unified SRST system and register itself.
6. Perform final configuration of buttons and numbers for the Cisco IP Communicator from the Cisco Unified SRST router.

DETAILED STEPS

Step 1 Download the latest version of the Cisco IP Communicator software and install it on your PC.

Step 2 (Optional) Attach a headset to your PC.

Step 3 Start the Cisco IP Communicator software application.

Step 4 Define the IP address of the Cisco Unified SRST TFTP server.

a. Open the Network > User Preferences window.

b. Enter the IP address of the Cisco Unified SRST TFTP server.

Step 5 Wait for the Cisco IP Communicator application to connect to the Cisco Unified SRST system and registers itself.

Verifying Cisco IP Communicator

Step 1 Use the **show running-config** command to display ephone-dn and ephone information associated with this phone.

Step 2 After Cisco IP Communicator registers with Cisco Unified CME, it displays the phone extensions and soft keys in its configuration. Verify that these are correct.

Step 3 Make a local call from the phone and ask someone to call you. Verify that you have a two-way voice path.

Troubleshooting Cisco IP Communicator

Use the **debug ephone detail** command to diagnose problems with calls. For more information, see the *Cisco IOS Debug Command Reference.*

Where to Go Next

The next step is setting up call handling. See the "Setting Up Call Handling" section on page 79 for instructions.

For additional information, see the "Additional References" section on page 46 in the Overview of Cisco Unified SRST chapter.

Setting Up Call Handling

Revised: July 11, 2008

This chapter describes how to configure Cisco Unified Survivable Remote Site Telephony (SRST) for incoming calls and outgoing calls.

Contents

Information About Setting Up Call Handling

Cisco Unified SRST offers a smaller set of call handling capabilities than Cisco Unified Communications Manager, and much of the configuration for these feature involves enabling existing Cisco Unified Communications Manager or Cisco Unified IP Phone settings.

How to Set Up Call Handling for Incoming and Outgoing Calls

Setting up call handling involves the following set of tasks:

- Configuring Incoming Calls, page 79
- Configuring Outgoing Calls, page 98

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 80 (Optional)
  - Configuring Call Rerouting, page 81 (Optional)

  - Configuring Call Pickup, page 84 (Optional)
  - Configuring Transfer Digit Collection Method, page 88
- Phone Number Conversion and Translation
  - Configuring Global Prefixes, page 89 (Optional)
  - Enabling Digit Translation Rules, page 91 (Optional)
  - Enabling Translation Profiles, page 92 (Optional)
  - Verifying Translation Profiles, page 95 (Optional)
- Hunting and Ringing Timeout Behavior
  - Configuring Dial-Peer and Channel Hunting, page 96 (Optional)
  - Configuring Busy Timeout, page 97 (Optional)
  - Configuring the Ringing Timeout Default, page 98 (Optional)

Configuring Call Forwarding During a Busy Signal or No Answer

Incoming calls that reach a busy signal or go unanswered during Cisco Unified Communications Manager 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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	`call-forward busy` *`directory-number`*
	Example:
	`Router(config-cm-fallback)# call-forward busy 50..`
		Configures call forwarding to another number when the Cisco IP phone is busy.
		• *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.

	Command or Action	Purpose

Step 3	**`call-forward noan`** *`directory-number`* **`timeout`** *`seconds`*
	Example:
	`Router(config-cm-fallback)# call-forward noan 5005 timeout 10`
		Configures call forwarding to another number when no answer is received from the Cisco IP phone.
		• *directory-number*: 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.
		• **timeout** *seconds*: Sets the waiting time, in seconds, before the call is forwarded to another phone. The *seconds* range is from 3 to 60000.

Step 4	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 seconds 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 seconds 15
```

Configuring Call Rerouting

Note The **alias** command obsoletes the **default-destination** command and is recommended over 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.

Note 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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`alias`** *`tag number-pattern`* **`to`** *`alternate-number`* `[`**`preference`** *`preference-value`*`]` `[`**`cfw`** *`number`* **`timeout`** *`timeout-value`*`]` `[`**`huntstop`**`]`
	Example:
	`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 Communications Manager 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.

	Command or Action	Purpose
Step 3	`max-dn` *max-directory-numbers* [`dual-line`] [`preference` *preference-order]* **Example:** `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.

Step 4	`end`
	Example:
	`Router(config-cm-fallback)# end`
		Returns to privileged EXEC mode.

Step 5	`show dial-peer voice summary`
	Example:
	`Router# show dial-peer voice summary`
		Displays information for voice dial peers.
		• If you suspect a problem with the dial peers, use this command to display the dial peers created by the **alias** command.

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 and Cisco 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 Communications Manager, 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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	`no huntstop`
	Example:
	`Router(config-cm-fallback)# no huntstop`
		Disables huntstop.

Step 3	**alias** *tag number-pattern* **to** *alternate-number* **Example:** `Router(config-cm-fallback)# alias 1 8005550100 to 5001`	Creates a set rules for rerouting calls to sets of phones that are unavailable during Cisco Unified Communications Manager 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.

	Command or Action	Purpose
Step 4	**pickup** *telephone-number* **Example:** `Router(config-cm-fallback)# pickup 8005550100`	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.

Step 5	**end**
	Example:
	`Router(config-cm-fallback)# end`
		Returns to privileged EXEC mode.

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.

```
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.

Note The new 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 88.

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. To configure call transfer features, see *Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide.*

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 Communications Manager 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

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 4	**`transfer-digit-collect`** {**`new-call`** | **`orig-call`**}
	Example:
	`Router(config-cm-fallback)# transfer-digit-collect orig-call`
		Selects the digit-collection method used for consultative call transfers.
		• **new-call**: Digits are collected from the new call leg. Default value.
		• **orig-call**: Digits are collected from the original call-leg. This was the default behavior in versions before Cisco Unified SRST 4.3.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`dialplan-pattern`** *`tag pattern`* **`extension-length`** *`length`* [**`extension-pattern`** *`extension-pattern`*] [**`no-reg`**] **Example:** `Router(config-cm-fallback)# dialplan-pattern 1 4085550100 extension-length 3 extension-pattern 4..` **Note** This example maps all extension numbers 4xx to the PSTN number 40855501xx, so that extension 412 corresponds to 4085550112.	Creates a global prefix that can be used to expand the abbreviated extension numbers into fully qualified E.164 numbers • *tag*: Dial-plan string tag used before a 10-digit telephone number. The tag number is from 1 to 5. • *pattern*: Dial-plan pattern, such as the area code, the prefix, and the first one or two digits of the extension number, plus wildcard markers or dots (.) for the remainder of the extension number digits. • **extension-length**: Sets the number of extension digits. • *length*:The number of extension digits. The range is from 1 to 32. • **extension-pattern**: (Optional) 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* argument. • *extension-pattern*: (Optional) The extension number's leading digit pattern. Consists of one or more digits and wildcard markers or dots (.). For example, 5.. would include extension 500 to 599; 5... would include 5000 to 5999. • **no-reg**: (Optional) Prevents the E.164 numbers in the dial peer from registering with the gatekeeper.

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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.

```
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.

```
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).

```
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 Communications Manager 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 the *Cisco IOS Voice Configuration Library.*

If you are running Cisco SRST 3.2 and later or Cisco Unified SRST and later, use the configuration described in the “Enabling Translation Profiles” section on page 92 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

	Command or Action	Purpose
Step 1	**call-manager-fallback** **Example:** `Router(config)# call-manager-fallback`	Enters call-manager-fallback configuration mode.
Step 2	**translate** {**called** | **calling**} *translation-rule-tag* **Example:** `Router(config-cm-fallback)# translate called 20`	Applies a translation rule to modify the phone number dialed or received by any Cisco Unified IP Phone user while Cisco Unified Communications Manager fallback is active. • **called**: Applies the translation rule to an outbound call number. • **calling**: Applies the translation rule to an inbound call number. • *translation-rule-tag*: The reference number of the translation rule from 1 to 2147483647.
Step 3	**exit** **Example:** `Router(config-cm-fallback)# exit`	Exits call-manager-fallback configuration mode.

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 Communications Manager 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 and Cisco Unified SRST 4.0 and later use the **voice translation-rule** and **translation-profile** commands shown below instead of the translation rule configuration described in "Enabling Digit Translation Rules" section on page 91. Voice translation rules are a separate feature from translation rules. See the **voice translation-rule** command in the *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

	Command or Action	Purpose
Step 1	**voice translation-rule** *number* **Example:** `Router(config)# voice translation-rule 1`	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.
Step 2	**rule** *precedence***/***match-pattern***/** **/***replace-pattern***/** **Example:** `Router(cfg-translation-rule)# rule 1/^9/ //`	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.
Step 3	**exit** **Example:** `Router(cfg-translation-rule)# exit`	Exits voice translation-rule configuration mode.
Step 4	**voice translation-profile** *name* **Example:** `Router(config)# voice translation-profile name1`	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.
Step 5	**translate** {**called** | **calling** | **redirect-called**} *translation-rule-number* **Example:** `Router(cfg-translation-profile)# translate called 1`	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.
Step 6	**exit** **Example:** `Router(cfg-translation-profile)# exit`	Exits translation-profile configuration mode.
Step 7	**call-manager-fallback** **Example:** `Router(config)# call-manager-fallback`	Enters call-manager-fallback configuration mode.

	Command or Action	Purpose
Step 8	**translation-profile** {**incoming** | **outgoing**} *name* **Example:** `Router(config-cm-fallback)# translation-profile outgoing name1`	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.
Step 9	**exit** **Example:** `Router(config-cm-fallback)# exit`	Exits call-manager-fallback configuration mode.

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.

```
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*]]

DETAILED STEPS

Step 1 **show voice translation-rule** *number*

Use this command to verify the translation rules that you have defined for your translation profiles.

```
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 **test voice translation-rule** *number input-test-string* [**type** *match-type* [**plan** *match-type*]]

Use this command to test your translation profiles. See the **test voice translation-rule** command in the *Cisco IOS Voice Command Reference* for more information.

```
Router(config)# voice translation-rule 5
Router(cfg-translation-rule)# rule 1 /201/ /102/
Router(cfg-translation-rule)# end
Router# test voice translation-rule 5 2015550101
Matched with rule 5
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 Communications Manager fallback by default. To enable dial-peer hunting, use the **no huntstop** command. For more information about dial-peer hunting, see the *Cisco IOS Voice Configuration Library*.

If you have a dual-line phone configuration (see the “Configuring Dual-Line Phones” section on page 72), you may want to 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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	`huntstop [channel]`
	Example:
	`Router(config-cm-fallback)# huntstop channel`
		Sets the huntstop attribute for the dial peers associated with the Cisco Unified IP Phone dial peers created during Communications Manager fallback.
		• 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.

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

Examples

The following example disables dial-peer hunting during Cisco Unified Communications Manager 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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	`timeouts busy` *seconds* **Example:** `Router(config-cm-fallback)# timeouts busy 20`	Sets the amount of time after which calls are disconnected when they are transferred to busy destinations. • *seconds*: Number of seconds. Range is from 0 to 30. Default is 10. **Note** 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.

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	`timeouts ringing` *`seconds`*
	Example:
	`Router(config-cm-fallback)# timeouts ringing 30`
		Sets the ringing timeout default, in seconds. The range is from 5 to 60000. There is no default value.

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

Examples

The following example sets the ringing timeout default to 30 seconds:

```
call-manager-fallback
 timeouts ringing 30
```

Configuring Outgoing Calls

Outgoing call configuration can include the following tasks:

- Configuring Call Transfer
  - Configuring Local and Remote Call Transfer, page 99 (Optional)
  - Enabling Consultative Call Transfer and Forward Using H.450.2 and H.450.3 with Cisco SRST 3.0, page 100 (Optional)
  - Enabling Analog Transfer Using Hookflash and the H.450.2 Standard with Cisco SRST 3.0 or Earlier, page 103 (Optional)

- Configuring Trunk Access Codes, page 107 (Required Under Certain Conditions)
- Configuring Interdigit Timeout Values, page 108 (Optional)
- Configuring Class of Restriction, page 109 (Optional)
- Call Blocking (Toll Bar) Based on Time of Day and Day of Week or Date, page 113 (Optional)

Configuring Local and Remote Call Transfer

You must configure Cisco Unified SRST to allow Cisco Unified IP Phones to transfer telephone calls from outside the local IP network to another Cisco Unified IP Phone. By default, all Cisco Unified IP Phone directory numbers or virtual voice ports are allowed as transfer targets. A maximum of 32 transfer patterns can be entered.

Call transfer configuration is performed using the **transfer-pattern** command.

SUMMARY STEPS

1. **call-manager-fallback**
2. **transfer-pattern** *transfer-pattern*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`transfer-pattern`** *`transfer-pattern`*
	Example:
	`Router(config-cm-fallback)# transfer-pattern 52540..`
		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.
		• *transfer-pattern*: String of digits for permitted call transfers. Wildcards are permitted.

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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

	Command or Action	Purpose
Step 1	**call-manager-fallback** **Example:** `Router(config)# call-manager-fallback`	Enters call-manager-fallback configuration mode.
Step 2	**call-forward pattern** *pattern* **Example:** `Router(config-cm-fallback)# call-forward pattern 4...`	Specifies the H.450.3 standard for call forwarding. • *pattern*: Digits to match for call forwarding using the H.450.3 standard. If an incoming calling-party number matches the pattern, it can be forwarded using the H.450.3 standard. A pattern of .T forwards all calling parties using the H.450.3 standard.

Step 3	**transfer-system** {**blind** | **full-blind** | **full-consult** | **local-consult**}
	Example:
	`Router(config-cm-fallback)# transfer-system full-consult`
		Not supported if the transfer-to destination is on the Cisco ATA, Cisco VG224, or a SCCP-controlled FXS port.
		Defines the call-transfer method for all lines served by the Cisco Unified SRST router.
		• **blind**: Calls are transferred without consultation with a single phone line using the Cisco proprietary method.
		Note The keyword **blind** is not recommended. Use either the **full-blind** or **full-consult** keyword instead.
		• **full-blind**: Calls are transferred without consultation using H.450.2 standard methods.
		• **full-consult**: Calls are transferred with consultation using a second phone line if available. The calls fall back to **full-blind** if the second line is unavailable.
		• **local-consult**: Calls are transferred with local consultation using a second phone line if available. The calls fall back to **blind** for nonlocal consultation or nonlocal transfer target.

Step 4	**transfer-pattern** *transfer-pattern* **Example:** `Router(config-cm-fallback)# transfer-pattern 52540..`	Allows transfer of telephone calls by Cisco Unified IP Phones to specified phone number patterns. • *transfer-pattern*: String of digits for permitted call transfers. Wildcards are allowed.
Step 5	**exit** **Example:** `Router(config-cm-fallback)# exit`	Exits call-manager-fallback configuration mode. **Timesaver** Before exiting call-manager-fallback configuration mode, configure any other parameters that you need to set for the entire Cisco Unified SRST phone network.

	Command or Action	Purpose
Step 6	**voice service voip** **Example:** `Router(config)# voice service voip`	(Optional) Enters voice service configuration mode.
Step 7	**h323** **Example:** `Router(conf-voi-serv)# h323`	(Optional) Enters H.323 voice service configuration mode.
Step 8	**h450 h450-2 timeout** {**T1** | **T2** | **T3** | **T4**} *milliseconds* **Example:** `Router(conf-serv-h323)# h450 h450-2 timeout T1 750`	(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. • **T1**:Timeout value to wait to identify a response. Default is 2000. • **T2**:Timeout value to wait for call setup. Default is 5000. • **T3**:Timeout value to wait to initiate a response. Default is 5000. • **T4**:Timeout value to wait for setup of a response. Default is 5000. • *milliseconds*: Number of milliseconds. Range is from 500 to 60000.

Step 9	**end**
	Example:
	`Router(conf-serv-h323)# end`
		(Optional) Returns to privileged EXEC mode.

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
!
```

```
dial-peer voice 4000 voip
 destination-pattern 4
 session-target ipv4:10.1.1.1
!
call-manager-fallback
 call-forward pattern 4
```

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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`call application voice` *`application-name location`*
	Example:
	`Router(config)# call application voice transfer_app flash:app-h450-transfer.tcl`
		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.

Step 2	`call application voice` *`application-name`* `language` *`number language`*
	Example:
	`Router(config)# call application voice transfer_app language 1 en`
		(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).

Step 3	`call application voice` *`application-name`* `set-location` *`language category location`*
	Example:
	`Router(config)# call application voice transfer_app set-location en 0 flash:/prompts`
		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.
		Prompts are required for call transfer from analog FXS phones. No prompts are needed for call transfer from IP phones.

	Command or Action	Purpose
Step 4	**call application voice** *application-name* **delay-time** *seconds* **Example:** `Router(config)# call application voice transfer_app delay-time 1`	(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.
Step 5	**dial-peer voice** *number* **pots** **Example:** `Router(config)# dial-peer voice 25 pots`	Enters dial-peer configuration mode to configure a POTS dial peer.
Step 6	**application** *application-name* **Example:** `Router(config-dial-peer)# application transfer_app`	Loads the application named in Step 1 onto the dial peer.
Step 7	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode. **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** **Example:** `Router(config)# dial-peer voice 29 voip`	Enters dial-peer configuration mode to configure a VoIP dial peer.
Step 9	**application** *application-name* **Example:** `Router(config-dial-peer)# application transfer_app`	Loads the application named in Step 1 onto the dial peer.
Step 10	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode. **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 Communications Manager fallback by creating POTS voice dial peers that are active during Cisco Unified Communications Manager 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 Communications Manager 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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**access-code** {{**fxo** | **e&m**} *dial-string* | {**bri** | **pri**} *dial-string* [**direct-inward-dial**]}
	Example:
	`Router(config-cm-fallback)# access-code e&m 8`
		Configures trunk access codes for each type of line so that the Cisco Unified IP Phones can access the trunk lines only in Cisco Unified Communications Manager fallback mode when the Cisco Unified SRST is enabled.
		• **fxo**: Enables a Foreign Exchange Office (FXO) interface.
		• **e&m**: Enables an analog Ear and Mouth (E&M) interface.
		• *dial-string*:String of characters that sets up dial access codes for each specified line type by creating dial peers. The *dial-string* argument is used to set up temporary dial peers for each specified line type.
		• **bri**: Enables a BRI interface.
		• **pri**: Enables a PRI interface.
		• **direct-inward-dial**: (Optional) Enables Direct Inward Dialing (DID) on the POTS dial peer.

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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.

Note This value setting is important when using variable-length dial-peer destination patterns (dial plans). For more information on setting dial plans, see the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

SUMMARY STEPS

1. **call-manager-fallback**
2. **timeouts interdigit** *seconds*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`timeouts interdigit`** *`seconds`*
	Example:
	`Router(config-cm-fallback)# timeouts interdigit 5`
		(Optional) Configures the interdigit timeout value for all Cisco IP phones that are attached to the router.
		- *seconds*:I nterdigit timeout duration, in seconds, for all Cisco Unified IP Phones. Valid entries are integers from 2 to 120.

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 Cisco Unified 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 1 describes call functionality based on how your COR lists are configured.

Table 1 Combinations of COR List and Results

COR List on Incoming Dial Peer	COR List on Outgoing Dial Peer	Result
No COR	No COR	Call will succeed.
No COR	COR list applied for outgoing calls	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.
COR list applied for incoming calls	No COR	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.
COR list applied for incoming calls (superset of COR list applied for outgoing calls on the outgoing dial peer)	COR list applied for outgoing calls (subsets of COR list applied for incoming calls on the incoming dial peer)	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.
COR list applied for incoming calls (subset of COR list applied for outgoing calls on the outgoing dial peer)	COR list applied for outgoing calls (supersets of COR list applied for incoming calls on the incoming dial peer)	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.

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

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**cor** {**incoming** | **outgoing**} *cor-list-name* [*cor-list-number starting-number* - *ending-number* | **default**] **Example:** `Router(config-cm-fallback)# cor outgoing LockforPhoneC 1 5010 - 5020`	Configures a COR on dial peers associated with directory numbers. • **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 20, comprised of incoming or outgoing dial peers. The first six COR lists are applied to a range of directory numbers. The directory numbers that do not have a COR configuration are assigned to the default COR list. • *starting-number - ending-number:* Directory number range; for example, 2000 - 2025. • **default**: Instructs the router to use an existing default COR list.

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 local_call

dial-peer cor list engineering
 member 911
 member local_call

dial-peer cor list manager
 member 911
 member 1800
 member 1900
 member local_call

dial-peer cor list hr
 member 911
 member 1800
 member local_call
```

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

dial-peer voice 2 voip
 destination pattern 1800.......
 session target ipv4:10.1.1.1
 cor outgoing call1800

dial-peer voice 3 pots
 destination pattern 1900.......
 port 1/0/0
 cor outgoing call1900

dial-peer voice 5 pots
 destination pattern 316....
 port 1/1/0
! No COR is applied.

dial-peer voice 4 pots
 destination pattern 911
 port 1/0/1
 cor outgoing call911
```

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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`after-hours block pattern`** *`tag pattern`* `[`**`7-24`**`]`
	Example:
	`Router(config-cm-fallback)# after-hours block pattern 1 91900`
		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.

	Command or Action	Purpose

Step 3	**`after-hours day`** *`day start-time stop-time`*
	Example:
	`Router(config-cm-fallback)# after-hours day mon 19:00 7:00`
		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."

Step 4	**`after-hours date`** *`month date start-time stop-time`*
	Example:
	`Router(config-cm-fallback)# after-hours date jan 1 0:00 0:00`
		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 an 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 5	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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., 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
```

H.323 VoIP Call Preservation Enhancements for WAN Link Failures

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 call agent is remote and therefore more likely to experience connectivity failures.

For configuration information see the "Configuring H.323 Gateways" chapter in the *Cisco IOS H.323 Configuration Guide*, Release 12.4T at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323confg/4gwconf.htm.

Where to Go Next

The next step is verifying whether you need to configure additional features available on Cisco Unified SRST. For a description and configuration instructions, see the "Configuring Additional Call Features" chapter. If you need to configure security, see the "Setting Up Secure SRST" chapter, or if you need to configure voicemail, see the"Integrating Voice Mail with Cisco Unified SRST" chapter. If you do not need any of those features, go to the "Monitoring and Maintaining Cisco Unified SRST" chapter.

For additional information, see the "Additional References" section on page 46 in the Overview of Cisco Unified SRST chapter.

Configuring Additional Call Features

Revised: July 11, 2008

This chapter 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.
- Integrating music on hold (MOH) for Cisco Unified Survivable Remote Site Telephony (SRST)—MOH is available from flash files on the Cisco Unified SRST router and for G.711, on-net VoIP, and PSTN calls. For more information about MOH, see the "Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource" section on page 121.

Contents

How to Configure Optional Features

The following sections describe how to configure these optional features:

- Enabling Three-Party G.711 Ad Hoc Conferencing, page 117
- Defining XML API Schema, page 119

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 72.

SUMMARY STEPS

1. **call-manager-fallback**
2. **max-conferences** *max-conference-numbers*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`max-conferences`** *`max-conference-numbers`*
	Example:
	`Router(config-cm-fallback)# max-conferences 16`
		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

Step 3	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 the *XML Provisioning Guide for Cisco CME/SRST.*

SUMMARY STEPS

1. **call-manager-fallback**
2. **xmlschema** *schema-url*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`xmlschema`** *`schema-url`*
	Example:
	`Router(config-cm-fallback)# xmlschema http://server2.example.com/ schema/schema1.xsd`
		Specifies the URL for an XML API schema to be used with this Cisco Unified SRST system.
		• *schema-url*: Local or remote URL as defined in RFC 2396.

Step 3	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

See the “Configuring Cisco Unified SRST MOH Live-Feed Support (Optional)” section on page 145 for configuration instructions.

Where to Go Next

For information about MOH, see the “Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource” section on page 121.

For information about monitoring and maintaining Cisco Unified SRST, see the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For related information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Integrating Cisco Unified Communications Manager and Cisco Unified SRST to Use Cisco Unified SRST as a Multicast MOH Resource

Revised: July 11, 2008

This chapter describes how to configure Cisco Unified Communications Manager and Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) to allow Cisco Unified Communications Manager to use Cisco Unified SRST gateways as multicast music-on-hold (MOH) resources during fallback and normal Cisco Unified Communications Manager 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 152.

Contents

Prerequisites for Using Cisco Unified SRST Gateways as a Multicast MOH Resource

- Multicast MOH for H.323 and MGCP is supported on Cisco Unified Communications Manager 3.1.1 and higher versions.
- Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager and Cisco Unified SRST must run on either H.323 or MGCP.
- For branches that do not run Cisco Unified SRST, Cisco Unified Communications Manager 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 the *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 the *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 Communications Manager 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.
- 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 Cisco 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 123
- Codecs, Port Numbers, and IP Addresses, page 124
- Multicast MOH Transmission, page 126
- Cisco Unified SRST MOH Live Feed Support, page 126

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 Communications Manager 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 Communications Manager.

Multicast MOH for PSTN callers is supported when the Cisco Unified SRST router is used as the Cisco IOS voice gateway for Cisco Unified Communications Manager. 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 Communications Manager 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 Communications Manager and the IP phones are spoofed and behave as if Cisco Unified Communications Manager were originating the multicast MOH.

Note Phone users at the central site would use multicast MOH from the central site.

Figure 1 Multicast MOH from Cisco Unified SRST Flash Memory

Codecs, Port Numbers, and IP Addresses

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 Communications Manager and three branches. In some cases, a Cisco Unified Communications Manager system may use additional codecs. For example, for bandwidth savings, Cisco Unified Communications Manager 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

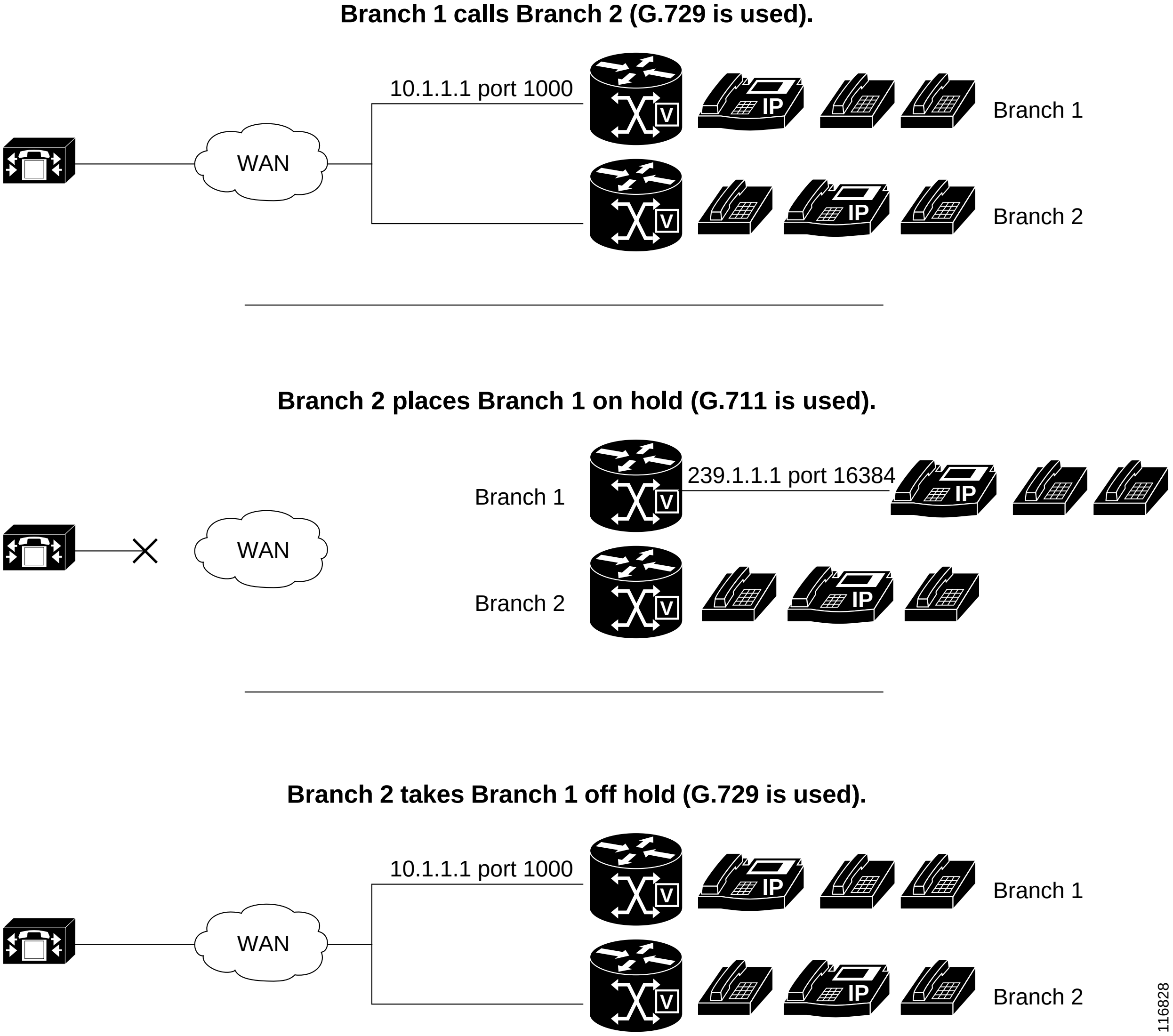

Branch 1 calls Branch 2 (G.729 is used).
10.1.1.1 port 1000
WAN
V
IP
Branch 1
Branch 2
Branch 2 places Branch 1 on hold (G.711 is used).
Branch 1
239.1.1.1 port 16384
Branch 2
WAN
Branch 2 takes Branch 1 off hold (G.729 is used).
10.1.1.1 port 1000
WAN
Branch 1
Branch 2
116828

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 Communications Manager system, MOH is originated by Cisco Unified Communications Manager. When Branch 1 and Branch 2 phone users are put on hold by other phone users in the Cisco Unified Communications Manager system, MOH is originated by the Cisco Unified SRST gateways.

Figure 3 MOH Sources for Cisco Unified SRST and Other Unified SRST IP Phones Using MOH

To enable MOH audio packet transmission through two paths, the Cisco Unified Communications Manager 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 Communications Manager 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” section on page 137.

Cisco Unified SRST MOH Live Feed Support

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 MOH Live-Feed Support (Optional)” section on page 145.

Configuring 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 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.

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 127
- Configuring Cisco Unified SRST for Multicast MOH, page 137
- Configuring Cisco Unified SRST MOH Live-Feed Support (Optional), page 145

Configuring Cisco Unified Communications Manager for Cisco Unified SRST Multicast MOH

The following sections describe the Cisco Unified Communications Manager configuration tasks for Cisco Unified SRST multicast MOH:

- Configuring the MOH Audio Source to Enable Multicasting, page 129
- Enabling Multicast on the Cisco Unified Communications Manager MOH Server and Configuring Port Numbers and IP Addresses, page 130
- Creating an MRG and an MRGL, Enabling MOH Multicast, and Configuring Gateways, page 133
- Creating a Region for the MOH Server, page 135
- Verifying Cisco Unified Communications Manager Multicast MOH, page 136

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 Communications Manager-sourced multicast MOH from actually reaching the WAN and the remote phones, the configured Cisco Unified Communications Manager MOH IP port and address information are still used by Cisco Unified Communications Manager 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 Communications Manager multicast MOH packets from reaching the WAN, thus spoofing Cisco Unified Communications Manager 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 Communications Manager 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.

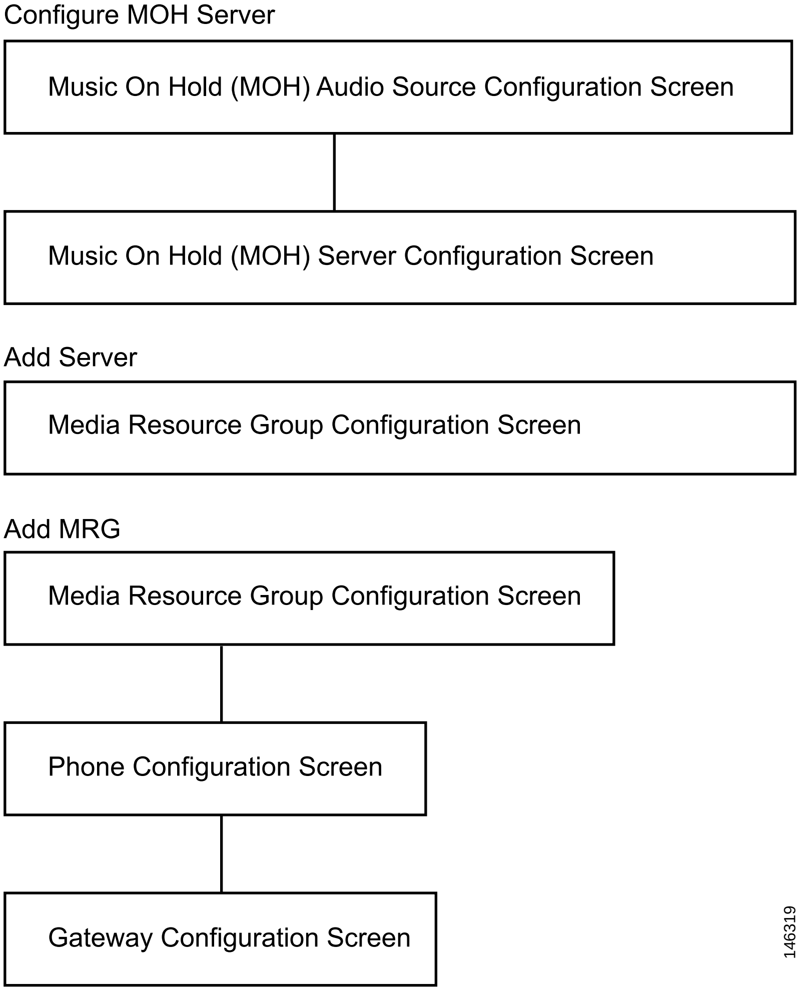
After the MOH server is configured, the MOH server must be added to a Media Resource Group (MRG); the MRG is added to a Media Resource Group List (MRGL); and the designated Cisco Unified Communications Manager branch gateways are configured to use the MRGL.

Five Cisco Unified Communications Manager 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 Communications Manager 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
146319

Configuring the MOH Audio Source to Enable Multicasting

The MOH audio source is a file from which Cisco Unified Communications Manager 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.

Tip The simplest way to create an audio source is to use the default audio source.

Whether you use a default Cisco Unified Communications Manager MOH audio source or you create one, the MOH audio source must be configured for multicasting in the Music On Hold (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 Communications Manager 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.

SUMMARY STEPS

1. Enable multicast MOH for the MOH audio source.
2. Enable the audio source.
3. Allow multicasting.
4. Apply all multicasting changes.

DETAILED STEPS

Step 1 To enable multicast MOH for the MOH audio source, choose **Service** > **Media Resources** > **Music On Hold Audio Source** to display the Music On Hold (MOH) Audio Source Configuration window.

Step 2 Double-click the required audio source listed in the MOH Audio Sources column.

Step 3 In the Music On Hold (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 Music On Hold (MOH) Server Configuration window. If you are using Cisco Unified Communications Manager multicast MOH and Cisco Unified SRST multicast MOH (see the “Codecs, Port Numbers, and IP Addresses” section on page 124 and the “Multicast MOH Transmission” section on page 126), 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 1 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.

Table 1 Example of the Differences Between Incrementing Multicast on IP Address and Incrementing Multicast on Port Number

		Increment Multicast on IP Address		Increment Multicast on Port Number	
Audio Source	Codec	Destination IP Address	Destination Port	Destination IP Address	Destination Port
1	G.711 mu-law	239.1.1.1	16384	239.1.1.1	16384
1	G.711 a-law	239.1.1.2	16384	239.1.1.1	16386
1	G.729	239.1.1.3	16384	239.1.1.1	16388
1	Wideband	239.1.1.4	16384	239.1.1.1	16390
2	G.711 mu-law	239.1.1.5	16384	239.1.1.1	16392
2	G.711 a-law	239.1.1.6	16384	239.1.1.1	16394
2	G.729	239.1.1.7	16384	239.1.1.1	16396
2	Wideband	239.1.1.8	16384	239.1.1.1	16398

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 1, 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 Communications Manager port number and IP address that use a G.711 audio source for Cisco Unified SRST multicast MOH. If Cisco Unified Communications Manager 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 Music On Hold (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 Communications Manager 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.

Use this procedure to enable multicast and configure port numbers and IP addresses.

SUMMARY STEPS

1. Enable multicast MOH for Cisco Unified Communications Manager.
2. Set the base IP address and port number.
3. Select whether Cisco Unified Communications Manager increments port numbers or IP addresses.
4. Enter a maximum number of hops.
5. Use Cisco IOS commands to stop Cisco Unified Communications Manager signals from crossing the WAN and reaching Cisco Unified SRST gateways.

DETAILED STEPS

Step 1 Enable multicast MOH for Cisco Unified Communications Manager.

a. Choose **Service** > **Media Resource** > **Music On Hold Server**.
b. The Music On Hold (MOH) Server Configuration window appears.
c. Call up an existing MOH server by clicking **Find** and double-clicking the required MOH server.
d. 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 Music On Hold (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 1.

Step 3 Select whether Cisco Unified Communications Manager increments port numbers or IP addresses.

In the Music On Hold (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 Music On Hold (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 Communications Manager 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:

a. **interface** {**serial** | **fastethernet**} *slot*/*port*

   Enters interface configuration mode, where *slot* is the slot number and *port* is the port number.

b. **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.

c. **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 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.

Use the following procedure to create an MRG and MRGL, to enable MOH multicast, and to configure gateways.

SUMMARY STEPS

1. Create an MRG with a multicast MOH media resource.
2. Create an MRGL that contains the newly created MRG.
3. Add the MRGL to the required IP phones.
4. Add the MRGL to the required gateway.

DETAILED STEPS

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 124. For information about regions, 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 Communications Manager version.

Configure the Region Configuration window. If the Cisco Unified Communications Manager 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 Communications Manager 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 doe 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.

SUMMARY STEPS

1. Create an MOH server region.
2. Create other regions as needed for different codecs.

DETAILED STEPS

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 Communications Manager multicast MOH configuration must run correctly in order 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 Communications Manager 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.

SUMMARY STEPS

1. Verify that Cisco Unified Communications Manager system’s multicast MOH is heard on a remote gateway.
2. Verify that Cisco Unified Communications Manager system’s MOH is multicast, not unicast.

DETAILED STEPS

Step 1 Verify that Cisco Unified Communications Manager 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 130). 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 Communications Manager 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

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 Communications Manager version. See the *Cisco Unified Communications Serviceability System Guide, Release 4.0(1)* for more information about RTMT.

Use the following procedure to configure Cisco Unified SRST for multicast MOH.

- Prerequisites, page 137
- Enabling Multicast MOH on the Cisco Unified SRST Gateway, page 138
- Verifying Basic Cisco Unified SRST Multicast MOH Streaming, page 141
- Verifying Cisco Unified SRST MOH to PSTN, page 142
- Verifying Cisco Unified SRST Multicast MOH to IP Phones, page 145
- Troubleshooting Tips, page 145

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.
- For Cisco Unified Communications Manager 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 Communications Manager.

  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

	Command or Action	Purpose

Step 1	`ccm-manager music-on-hold`
	Example:
	`Router(config)# ccm-manager music-on-hold`
		Enables the multicast MOH feature on a voice gateway.

Step 2	`interface loopback` *`number`*
	Example:
	`Router(config)# interface loopback 1`
		Configures an interface type and enters the interface configuration mode.
		• *number*—Loopback interface number. The range is from 0 to 2147483647.

	Command or Action	Purpose

Step 3	**`ip address`** *`ip-address mask`*
	Example:
	`Router(config-if)# ip address 10.1.1.1 255.255.255.255`
		Sets a primary IP address for an interface.
		• *ip-address*—IP address.
		• *mask*—Mask for the associated IP subnet.

Step 4	**`exit`**
	Example:
	`Router(config-if)# exit`
		Exits interface configuration mode.

Step 5	**`interface fastethernet`** *`slot`*`/`*`port`*
	Example:
	`Router(config)# interface fastethernet 0/0`
		(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.

Step 6	**`ip address`** *`ip-address mask`*
	Example:
	`Router(config-if)# ip-address 172.21.51.143 255.255.255.192`
		(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.

Step 7	**`exit`**
	Example:
	`Router(config-if)# exit`
		(Optional if the **route** keyword is not used in the **multicast moh** command. See Step 9 and Step 13.) Exits interface configuration mode.

Step 8	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 9	**`ip source-address`** *`ip-address`* `[`**`port`** *`port`*`]`
	Example:
	`Router(config-cm-fallback)# ip source-address 172.21.51.143 port 2000`
		(Optional if the **route** keyword is not used in the **multicast moh** command. See Step 13.) Enables a router to receive messages from Cisco Unified IP phones through the specified IP addresses and ports.
		• *ip-address*—The preexisting 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 the Cisco Unified IP phones. The port number range is from 2000 to 9999. The default port number is 2000.

Step 10	**`max-ephones`** *`max-phones`*
	Example:
	`Router(config-cm-fallback)# max-ephones 1`
		Configures the maximum number of Cisco Unified IP phones that can be supported by a router.
		• *max-phones*—Maximum number of Cisco IP phones supported by the router. The maximum number is platform-dependent. The default is 0.

	Command or Action	Purpose

Step 11	`max-dn max-directory-number`
	Example:
	`Router(config-cm-fallback)# max-dn 1`
		Sets the maximum possible number of virtual voice ports that can be supported by a router.
		- *max-directory-number*—Maximum number of directory numbers or virtual voice ports supported by the router. The maximum possible number is platform-dependent. The default is 0.

Step 12	`moh filename`
	Example:
	`Router(config-cm-falback)# moh music-on-hold.au`
		Enables use of an MOH file.
		- *filename*—Filename of the music file. The music file must reside in flash memory.

Step 13	`multicasting-enabled`	Selects the multicast-enabled MOH audio source in the User Hold MOH Audio Source field on the Phone Configuration page in Cisco Unified Communications Manager Administration GUI.

Step 14	`multicast moh multicast-address port port [route ip-address-list]`
	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`
		Enables multicast of MOH from a branch office flash MOH file to IP phones in the branch office.
		- *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, instead an incremented IP address or port number. See the "Configuring the MOH Audio Source to Enable Multicasting" section on page 129. If you have multiple audio sources configured on Cisco Unified Communications Manager, ensure that you are using the audio sources's 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.

Step 15	`exit`
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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**

DETALED STEPS

Step 1 **debug ephone moh**

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:

```
Router# debug ephone moh
!
MOH route If FastEthernet0/0 ETHERNET 172.21.51.143 via ARP
MOH route If Loopback0 46 172.21.51.98 via 172.21.51.98
!
```

Step 2 **show interfaces fastethernet**

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.

```
Router# show interfaces fastethernet 0/0
!
30 second output rate 86000 bits/sec, 50 packets/sec
!
```

Step 3 **show ephone summary**

Use this command to verify that the Cisco IOS software was able to read the MOH audio file successfully.

```
Router# show ephone summary
!
File music-on-hold.au type AU Media_Payload_G.711Ulaw64k  160 bytes
!
```

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 Communications Manager control of MOH (the WAN link is up) and that multicast MOH packets transmit over a public switched telephone network (PSTN).

Note This feature does not apply when the Cisco Unified SRST router is in fallback mode.

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

Step 1 Verify that a PSTN caller hears MOH when placed on hold by an IP phone caller.

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.

Step 2 **show ccm-manager music-on-hold**

Use this command to verify that the MOH is multicast if you are using Windows and Cisco Unified Communications Manager version 4.3 or an earlier version. Note that 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. The following is an example of **show ccm-manager music-on-hold** command output.

```
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 the PSTN caller hears MOH, and the **show ccm-manager music-on-hold** 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 136.

Step 3 **debug h245 asn**

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.

```
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 : iPAddress :
        {
          network 'EF010101'H
          tsapIdentifier 16384
        }
        mediaControlChannel unicastAddress : iPAddress :
        {
          network 'EF010101'H
          tsapIdentifier 16385
        }
      }
    }
```

Step 4 **show call active voice**

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.

```
Router# show call active voice | include RemoteMedia

RemoteMediaIPAddress=239.1.1.1
RemoteMediaPort=16384
```

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 122.

Troubleshooting Tips

- If the PSTN caller hears tone on hold (TOH) instead of MOH, two problems are probable:
  - Cisco Unified Communications Manager 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 136.
  - Cisco Unified Communications Manager 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.

Note 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 Communications Manager 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 Communications Manager 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 Communications Manager (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 Communications Manager region for incorrect codec configuration. See the "Creating a Region for the MOH Server" section on page 135.
  - 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 138.

Verifying Cisco Unified SRST Multicast MOH to IP Phones

To verify that Cisco Unified Communications Manager is signaling the IP phone to receive Cisco Unified SRST multicast MOH correctly, perform the following steps.

SUMMARY STEPS

1. Verify that an IP phone caller hears MOH when placed on hold by an IP phone caller.
2. Check the MOHMulticastResourceActive and MOHUnicastResourceActive counters.

DETAILED 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 136. 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 MOH Live-Feed Support (Optional)

The following sections describe the configuration tasks for Cisco Unified SRST MOH live feed:

- Prerequisites, page 146
- Restrictions, page 146
- Setting Up the Voice Port on the Cisco Unified SRST Gateway, page 147
- Setting Up the Directory Numbers on the Cisco Unified SRST Gateway, page 148
- Establishing the MOH Feed, page 149

- Verifying Cisco Unified SRST MOH Live Feed, page 151

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.

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 "Configuring Cisco Unified SRST for Multicast MOH" section on page 137, 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.

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

	Command or Action	Purpose
Step 1	`voice-port` *port* **Example:** `Router(config)# voice-port 1/1/0`	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 the *Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference*.
Step 2	`input gain` *decibels* **Example:** `Router(config-voice-port)# input gain 0`	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.

Step 3	`auto-cut-through`
	Example:
	`Router(config-voiceport)# auto-cut-through`
		(E&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&M ports.

Step 4	`operation 4-wire`
	Example:
	`Router(config-voiceport)# operation 4-wire`
		(E&M ports only) Selects the 4-wire cabling scheme. MOH requires that you specify 4-wire operation with this command for E&M ports.

Step 5	`signal immediate`
	Example:
	`Router(config-voiceport)# signal immediate`
		(E&M ports only) For E&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.

	Command or Action	Purpose

Step 6	`no shutdown`
	Example:
	`Router(config-voiceport)# no shutdown`
		Activates the voice port.

Step 7	`exit`
	Example:
	`Router(config-voiceport)# exit`
		Exits voice-port configuration mode.

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

	Command or Action	Purpose

Step 1	**`dial-peer voice`** *`tag`* **`pots`**
	Example:
	`Router(config)# dial-peer voice 7777 pots`
		Enters dial-peer configuration mode.

Step 2	**`destination-pattern`** *`string`*
	Example:
	`Router(config-dial-peer)# destination-pattern 7777`
		Specifies the directory number that the system uses to create music on hold. This command specifies either the prefix or the full E.164 telephone number to be used for a dial peer.

Step 3	**`port`** *`port`*
	Example:
	`Router(config-dial-peer)# port 1/1/0`
		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 147.

Step 4	`exit`
	Example:
	`Router(config-dial-peer)# exit`
		Exits dial-peer configuration mode.

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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`max-dn`** *`max-directory-number`*
	Example:
	`Router(config-cm-fallback)# max-dn 1`
		Sets the maximum possible number of virtual voice ports that can be supported by a router.
		• *max-directory-number*—Maximum number of directory numbers or virtual voice ports supported by the router. The maximum possible number is platform-dependent. The default is 0.

	Command or Action	Purpose
Step 3	`multicast moh` *multicast-address* `port` *port* [`route` *ip-address-list*] **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`	Enables multicast of MOH from a branch office flash MOH file to IP phones in the branch office. **Note** This command must be used to source live feed MOH to multicast Cisco Unified Communications Manager 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 129. If you have multiple audio sources configured on Cisco Unified Communications Manager, 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.
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 147 .

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 141.

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 151
- MOH Live Feed: Example, page 151

MOH Routed to Two IP Addresses: Example

The following example declares the Cisco Unified Communications Manager 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
 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 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 129. If you have multiple audio sources configured on Cisco Unified Communications Manager, 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
!
!
moh filename
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 2 lists the enhancements to the Cisco Unified SRST as a Mulitcast MOH Resource feature by version.

To determine hardware and software compatibility, see the Cisco Unified Communications Manager Compatibility Information page at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

See also the Cisco Unified Communications Manager Documentation Roadmaps at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.htm.

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.

Note Table 2 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 2 *Feature Information for* **Cisco Unified SRST as a Multicast MOH Resource**

Feature Name	Releases	Feature Information
Cisco Unified SRST as a Multicast MOH Resource	3.0	The MOH-live feature was added.

Where to Go Next

For information about monitoring and maintaining Cisco Unified SRST, see the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Setting Up Secure SRST

Revised: July 11, 2008

This chapter describes new Secure SRST security features such as authentication, integrity, and media encryption.

Contents

Prerequisites for Setting Up Secure SRST

General

- Secure Cisco Unified IP phones supported in secure SRST must have certificates installed and encryption enabled.
- 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.
- Cisco Unified Communications Manager 4.1(2) or later must be installed and must support security mode (authenticate and encryption mode).
- Certificate trust lists (CTLs) on Cisco Unified Communications Manager must be enabled. For complete instructions, see the "Configuring Secure IP Telephony Calls" procedure in the *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* document.
- Gateway routers that run secure SRST must support voice- and security-enabled Cisco IOS images (a "k9" cryptographic software image). The following two images are supported:
  - Advanced IP Services. This image includes a number of advanced security features.
  - Advanced Enterprise Services. This image includes full Cisco IOS software.

Public Key Infrastructure

- 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.

SRST

- Secure SRST services cannot be enrolled while Cisco Unified SRST is active. Therefore, disable Cisco Unified SRST with the **no call-manager-fallback** 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 *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* 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 4.3 Supported Firmware, Platforms, Memory, and Voice Products* feature.

Restrictions for Setting Up 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:
  http://www.cisco.com/wwl/export/crypto/tool/

  If you require further assistance, please contact us by sending e-mail to export@cisco.com.
- 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.

- Secure SRST is supported only within the scope of a single router.

Not Supported in Secure SRST Mode

- Cisco Unified Communications Manager versions prior to 4.1(2)
- Secure music on hold (MoH); MoH stays active, but reverts to non-secure.
- Secure transcoding or conferencing
- Secure H.323 or SIP trunks
- SIP phones interoperability.
- Hot Standby Routing Protocol (HSRP)

Supported Calls in Secure SRST Mode

Only voice calls are supported in secure 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

Information About Setting Up Secure SRST

To configure secure SRST, you should understand the following concepts:

- Benefits of Secure SRST, page 155
- Cisco IP Phones Clear-Text Fallback During SRST, page 156
- SRST Routers and the TLS Protocol, page 156
- Cisco Unified SRST Routers and PKI, page 156
- Secure SRST Authentication and Encryption, page 157
- Cisco IOS Credentials Server on Secure SRST Routers, page 159
- Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone, page 159

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 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 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.

Cisco IP Phones Clear-Text Fallback During SRST

Cisco Unified SRST versions prior to 12.3(14)T are not capable of supporting secure connections or have security enabled. If an SRST router is not capable of secure 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 the *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for more information on clear-text mode.

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 fallback 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.

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 1 shows the secure SRST-supported Cisco Unified IP Phones and the appropriate certificate for each phone. The “Importing Phone Certificate Files in PEM Format to the Secure SRST Router” section on page 170 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 1 Supported Cisco Unified IP Phones and Certificates

Cisco Unified IP Phone 7940	Cisco Unified IP Phone 7960	Cisco Unified IP Phone 7970
The phone receives locally significant certificate (LSC) from Certificate Authority Proxy Function (CAPF) in Distinguished Encoding Rules (DER) format. • 59fe77ccd.0 The filename may change based on the CAPF certificate subject name and the CAPF certificate issuer. If Cisco Unified Communications Manager is using a third-party certificate provider, there can be multiple .0 files (from two to ten). Each .0 certificate file must be imported individually during the configuration. Manual enrollment supported only.	The phone receives locally significant certificate (LSC) from Certificate Authority Proxy Function (CAPF) in Distinguished Encoding Rules (DER) format. • 59fe77ccd.0 The filename may change based on the CAPF certificate subject name and the CAPF certificate issuer. If Cisco Unified Communications Manager is using a third-party certificate provider, there can be multiple .0 files (from two to ten). Each .0 certificate file must be imported individually during the configuration. Manual enrollment supported only.	The phone contains a manufacturing installed certificate (MIC) used for device authentication. If the Cisco 7970 implements MIC, two public certificate files are needed: • CiscoCA.pem (Cisco Root CA, used to authenticate the certificate.) **Note** The name of the manufacturing certificate can vary depending on your configuration. • a69d2e04.0, in Privacy Enhanced Mail (PEM) format If Cisco Unified Communications Manager is using a third-party certificate provider, there can be multiple .0 files (from two to ten). Each .0 certificate file must be imported individually during the configuration. Manual enrollment supported only.

Secure SRST Authentication and Encryption

Figure 1 illustrates the process of secure SRST authentication and encryption, and Table 2 describes the process.

Figure 1 Secure Cisco Unified SRST Authentication and Encryption

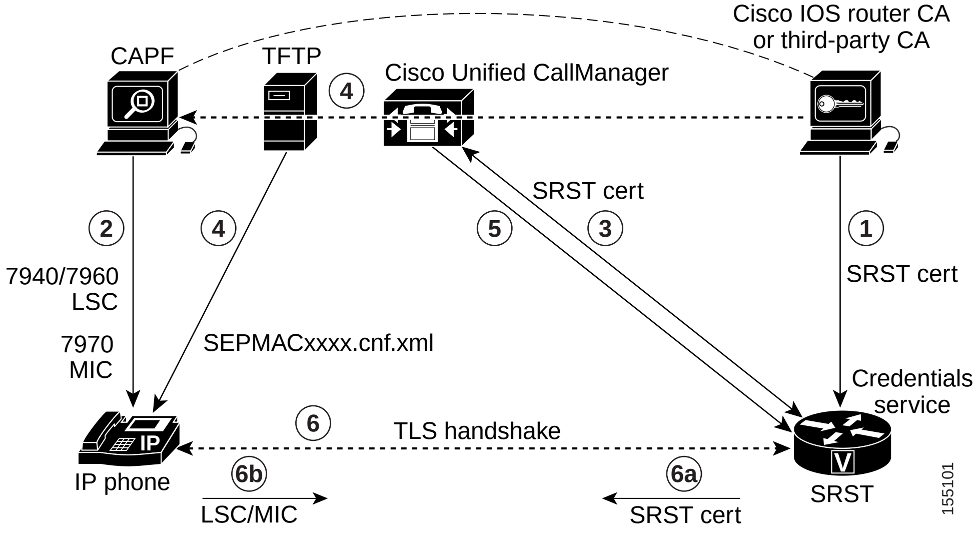


Table 2 Overview of the Process of Secure SRST Authentication and Encryption

Process Steps	Description or Detail
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 the *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.
4.	For each device, Cisco Unified Communications Manager uses the TFTP process and inserts the certificate into the SEPMACxxxx.cnf.xml configuration file of the Cisco Unified IP Phone.
5.	Cisco Unified Communications Manager 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 Unified SRST Routers and PKI, page 156 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.

Table 2 Overview of the Process of Secure SRST Authentication and Encryption (continued)

Process Steps	Description or Detail
6.	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.
a.	The Cisco Unified SRST Router sends its certificate, and the phone validates the certificate to the certificate that it received from Cisco Unified Communications Manager in Step 4.
b.	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.

Note The media is encrypted automatically after the phone and router certificates are exchanged and the TLS connection is established with the SRST router.

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

Establishment of Secure Cisco Unified SRST to the Cisco Unified IP Phone

Figure 2 and Table 3 show the interworking of the credentials server on the SRST router, Cisco Unified Communications Manager, and the Cisco Unified IP Phone, and describe the establishment of secure SRST to the Cisco Unified IP Phone.

Figure 2 Interworking of Credentials Server on SRST Router, Cisco Unified Communications Manager, and Cisco Unified IP Phone

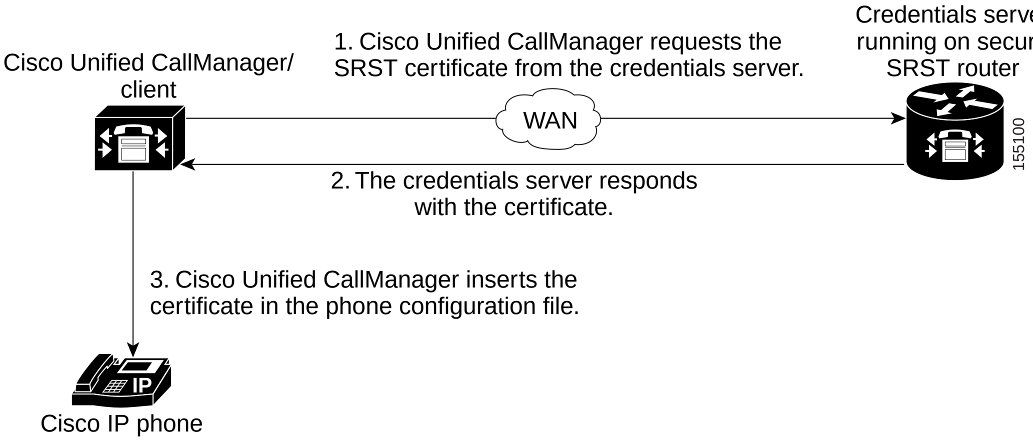

Cisco Unified CallManager/
client
1. Cisco Unified CallManager requests the
SRST certificate from the credentials server.
Credentials server
running on secure
SRST router
WAN
155100
2. The credentials server responds
with the certificate.
3. Cisco Unified CallManager inserts the
certificate in the phone configuration file.
IP
Cisco IP phone

Table 3 Establishing Secure SRST

Mode	Process	Description or Detail
Regular Mode	The Cisco Unified IP Phone configures DHCP and gets the TFTP server address.	—
	The Cisco Unified IP Phone retrieves a CTL file from the TFTP server.	The CTL file contains the certificates that the phone should trust.
	The Cisco IP Phone opens a Transport Layer Security (TLS) protocol channel and registers to Cisco Unified Communications Manager.	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 2.
	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.	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 2. Cisco Unified Communications Manager should be configured in mixed mode, which is its secure mode.
In case of WAN failure, the Cisco Unified IP Phone starts Cisco Unified SRST registration.		
SRST Mode	The Cisco Unified IP Phone registers with the SRST router at the default port for secure communications.	—

How to Configure Secure 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 161 (required)
- Importing Phone Certificate Files in PEM Format to the Secure SRST Router, page 170 (required)
- Configuring Cisco Unified Communications Manager to the Secure Cisco Unified SRST Router, page 177 (required)
- Enabling SRST Mode on the Secure Cisco Unified SRST Router, page 180 (required)
- Verifying Phone Status and Registrations, page 182 (required)

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 161 (optional)
- Autoenrolling and Authenticating the Secure Cisco Unified SRST Router to the CA Server, page 163 (required)
- Disabling Automatic Certificate Enrollment, page 165 (required)
- Verifying Certificate Enrollment, page 166 (optional)
- Enabling Credentials Service on the Secure Cisco Unified SRST Router, page 168 (required)
- Troubleshooting Credential Settings, page 169 (optional)

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

	Command or Action	Purpose
Step 1	**crypto pki server** *cs-label* **Example:** `Router (config)# crypto pki server srstcaserver`	Enables the certificate server and enters certificate server configuration mode. **Note** If you manually generated an RSA key pair, the *cs-label* argument must match the name of the key pair. For more information on the certificate server, see the *Cisco IOS Certificate Server* documentation.

Step 2	**database level** {**minimal** | **names** | **complete**}
	Example:
	`Router (cs-server)# database level complete`
		Controls what type of data is stored in the certificate enrollment database.
		• **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 via the **database url** command.

Step 3	**database url** *root-url* **Example:** `Router (cs-server)# database url nvram`	Specifies the location where all database entries for the certificate server will be written. After you create a certificate server via 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. • 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* **Example:** `Router (cs-server)# issuer-name CN=srstcaserver`	Sets the CA issuer name to the specified distinguished name (DN-string). The default value is as follows: **issuer-name CN**=*cs-label*.

	Command or Action	Purpose
Step 5	**grant auto** **Example:** `Router (cs-server)# grant auto`	Allows an automatic certificate to be issued to any requestor. • This command is used only during enrollment and will be removed in the "Disabling Automatic Certificate Enrollment" section on page 165.
Step 6	**no shutdown** **Example:** `Router (cs-server)# no shutdown`	Enables the Cisco IOS certificate server. • You should issue this command only after you have completely configured your certificate server.

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 165.

SUMMARY STEPS

1. **crypto pki trustpoint** *name*
2. **enrollment url** *url*
3. **revocation-check** *method1*
4. **exit**

5. **crypto pki authenticate** *name*
6. **crypto pki enroll** *name*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`crypto pki trustpoint`** *`name`*
	Example:
	`Router(config)# crypto pki trustpoint srstca`
		Declares the CA that your router should use and enters ca-trustpoint configuration mode.
		• 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 168.

Step 2	**`enrollment url`** *`url`*
	Example:
	`Router(ca-trustpoint)# enrollment url http://10.1.1.22`
		Specifies the enrollment parameters of your CA.
		• **url** *url*: Specifies the URL of the CA to which your router should send certificate requests.
		• If you are using Cisco proprietary SCEP for enrollment, *url* must be in the form http://*CA_name*, where *CA_name* is the host Domain Name System (DNS) name or IP address of the Cisco IOS CA.
		• If you used the procedure documented in the "Configuring a Certificate Authority Server on a Cisco IOS Certificate Server" section on page 161, 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.

Step 3	**`revocation-check`** *`method1`*
	Example:
	`Router(ca-trustpoint)# revocation-check none`
		Checks the revocation status of a certificate. The argument *method1* is the method used by the router to check the revocation status of the certificate. For this task, the only available method is **none.** The keyword **none** means that a revocation check will not be performed and the certificate will always be accepted.
		• Using the **none** keyword is mandatory for this task.

Step 4	**`exit`**
	Example:
	`Router(ca-trustpoint)# exit`
		Exits ca-trustpoint configuration mode and returns to global configuration mode.

Step 5	**`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 6	**`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.

```
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 58DA618A 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 MD5: D154FB75
2524A24D 3D1F5C2B 46A7B9E4
Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 0573FBB2
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 161.

Note A security best practice is to 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

	Command or Action	Purpose
Step 1	**crypto pki server** *cs-label* **Example:** `Router (config)# crypto pki server srstcaserver`	Enables the certificate server and enters certificate server configuration mode. **Note** If you manually generated an RSA key pair, the *cs-label* argument must match the name of the key pair.
Step 2	**shutdown** **Example:** `Router (cs-server)# shutdown`	Disables the Cisco IOS certificate server.
Step 3	**no grant auto** **Example:** `Router (cs-server)# no grant auto`	Disables automatic certificates to be issued to any requestor. • This command was for use during enrollment only and thus needs to be removed in this task.
Step 4	**no shutdown** **Example:** `Router (cs-server)# no shutdown`	Enables the Cisco IOS certificate server. • 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**

DETAILED STEPS

Step 1 **show running-config**

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.

```
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 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
  32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
  C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
  FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
  03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
  06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
  CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
  FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
  B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
  C3AF4A66 BD007348 D013000A EA3C206D CF
  quit
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
  55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
  1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
  9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
  47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
  C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
  DEDBAAD7 3780136E B112A6
  quit
```

Step 2 **show crypto pki server**

Use the **show crypto pki server** command to verify the status of the CA server after a boot procedure.

```
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
CA certificate expiration timer: 13:46:57 PST Dec 1 2007
CRL NextUpdate timer: 14:54:57 PST Jan 19 2005
Current storage dir: nvram
Database Level: Complete - all issued certs written as <serialnum>.cer
```

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.

Note 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 192.

SUMMARY STEPS

1. **credentials**
2. **ip source-address** *ip-address* [**port** *port*]
3. **trustpoint** *trustpoint-name*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`credentials`
	Example:
	`Router(config)# credentials`
		Provides the Cisco Unified SRST Router certificate to Cisco Unified Communications Manager and enters credentials configuration mode.

Step 2	`ip source-address` *`ip-address`* `[port` *`port`*`]`
	Example:
	`Router(config-credentials)# ip source-address 10.1.1.22 port 2445`
		Enables the Cisco Unified SRST Router to receive messages from Cisco Unified Communications Manager through the specified IP address and port.
		• *ip-address*: The IP address is the preexisting 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.

	Command or Action	Purpose
Step 3	**trustpoint** *trustpoint-name* **Example:** `Router(config-credentials)# trustpoint srstca`	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. • 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 163.
Step 4	**exit** **Example:** `Router(config-credentials)# exit`	Exits credentials configuration mode.

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

Step 1 **show credentials**

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.

```
Router# show credentials

Credentials IP: 10.1.1.22
Credentials PORT: 2445
Trustpoint: srstca
```

Step 2 **debug credentials**

Use the **debug credentials** command to set debugging on the credential settings of the Cisco Unified SRST Router.

```
Router# debug credentials

Credentials server debugging is enabled
Router#
```

```
Sep 29 01:01:50.903: Credentials service: Start TLS Handshake 1 10.1.1.13 2187
Sep 29 01:01:50.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:51.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:52.907: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:53.927: Credentials service: TLS Handshake completes.
```

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 provisioning tasks required of 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 1 on page 157 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.

Cisco Unified Communications Manager 5.0 and Later Versions

Systems running Cisco Unified Communications Manager 5.0 and later versions require four certificates (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) in addition to the requirements listed in Table 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
```

Cisco Unified Communications Manager 4.X.X and Earlier Versions

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 of the contents that appear between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”.

Cisco Unified Communications Manager 5.0 and Later Versions

For Cisco Unified Communications Manager 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.

Step 8 Copy all of 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.

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** *method1*
3. **enrollment terminal**
4. **exit**
5. **crypto pki authenticate** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**crypto pki trustpoint** *name* **Example:** `Router (config)# crypto pki trustpoint 7970`	Declares the CA that your router should use and enters ca-trustpoint configuration mode. • If you are using Cisco Unified Communications Manager 5.0, you must configure four *name* arguments (CAPF, CiscoCA, CiscoManufactureCA, and CiscoRootCA2048) individually. See the "Cisco Unified Communications Manager 5.0 and Later Versions Example" section on page 175.
Step 2	**revocation-check** *method1* **Example:** `Router(ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate. The argument *method1* is the method used by the router to check the revocation status of the certificate. For this task, the only available method is **none.** The keyword **none** means that a revocation check will not be performed and the certificate will always be accepted. • Using the **none** keyword is mandatory for this task.
Step 3	**enrollment terminal** **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment.
Step 4	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration.
Step 5	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate 7970`	Authenticates the CA (by getting the certificate from the CA). • Enter the same *name* argument used in the **crypto pki trustpoint** command.

Examples

This section provides the following:

- Cisco Unified Communications Manager 4.X.X and Earlier Versions Example, page 172
- Cisco Unified Communications Manager 5.0 and Later Versions Example, page 175

Cisco Unified Communications Manager 4.X.X and Earlier Versions Example

The following example shows three certificates imported to the Cisco Unified SRST Router (Cisco 7970, 7960, PEM).

```
Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7970
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCCApCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAyMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEAxCZlBK19w/2NZVVvpjCPrpW1cCY7V1q9lhzI85RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcRECnMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uhtl
AVVf5NQgZ3YDNoNXg5MmONb8lT86F55EZyVac0XGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQlGFDRzbHfM84Duv2Msez+l+SqmqO80kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+sj9+F6KKK2PD0iDwHcRKkcUHb7g
lI++U/5nswjUDIAph715Ds2rn9ehkMGipGLF8kpuCwIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAyL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDIuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMlxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdwMS5JaqUtuaSd/m/xzxpcRJm4ZRRwPq6VeaiiQGkjFuZEe5jSKiSAK7eHg
tup4HP/ZfKSwPA40DlsGSYsKNMm3OmVOCQUMH02lPkS/eEQ9sIw6QS7uuHN4y4CJ
NPnRbpFRLw06hnStCZHtGpKEHnY213QOy3h/EWhbnp0MZ+hdr20FujSI6G1+L39l
aRjeD708f2fYoz9wnEpZbtn2Kzse3uhU1Ygq1D1x9yuPq388C18HWdmCj4OVTXux
V6Y47H1yv/GJM8FvdgvKlExbGTFnlHpPiaG9tQ==
quit
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(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7960

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKDCCAZGgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQDELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRUwEwYDVQQDEwxDQVBGLTdEN0Qw
QzAwHhcNMDQwNzE1MjIzODMyWhcNMTkwNzEyMjIzODMxWjBAMQswCQYDVQQGEwJV
UzEaMBgGA1UEChMRQ2lzY28gU3lzdGVtcyBJbmMxFTATBgNVBAMTDENBUEYtN0Q3
RDBDMDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0hvMOZZ9ENYWme11YGY1
it2rvE3Nk/eqhnv8P9eqB1iqt+fFBeAG0WZ5bO5FetdU+BCmPnddvAeSpsfr3Z+h
x+r58fOEIBRHQLgnDZ+nwYH39uwXcRWWqWwlW147YHjV7M5c/R8T6daCx4B5NBo6
kdQdQNOrV3IP7kQaCShdM/kCAwEAAaMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBgQCaNi6x
sL6M5NlDezpSBO3QmUVyXMfrONV2ysrSwcXzHu0gJ9MSJ8TwiQmVaJ47hSTlF5a8
YVYJ0IdifXbXRo+/EEO7kkmFE8MZta5rM7UWj8bAeR42iqA3RzQaDwuJgNWT9Fhh
GgfuNAlo5h1AikxsvxivmDlLdZyCMoqJJd7B2Q==
quit
Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DBC
Fingerprint SHA1: A9917775 F86BB37A 5C130ED2 3E528BB8 286E8C2D
% 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)# enrollment terminal
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
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Fw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzM2MzRaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAxMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEArFW77Rjem4cJ/7yPLVCauDohwZZ/3qf0sJaWlLeAzBlq
Rj2lFlSij0ddkDtfEEo9VKmBOJsvx6xJlWJiuBwUMDhTRbsuJz+npkaGBXPOXJmN
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEdHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZXmeHjqEgVO3UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxwlANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6Rexgscfz6ypG270qSac
cK4FoJowbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAxL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDEuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMVxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAxLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAq2T96/YMMtw2Dw4QX+F1+g1XSrUCrNyjx7vtFaRDHyB+kobw
dwkpohfkzfTyYpJELzV1r+kMRoyuZ7oIqqccEroMDnnmeApc+BRGbDJqS1Zzk4OA
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrcxb0UH7IQJ1ogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
quit
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

Trustpoint 7970:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-002,o=Cisco Systems
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
State:
Keys generated ............. Yes (General Purpose)
Issuing CA authenticated ....... Yes
Certificate request(s) ..... None

Trustpoint 7960:
Issuing CA certificate configured:
Subject Name:
cn=CAPF-508A3754,o=Cisco Systems Inc,c=US
Fingerprint MD5: 6BAE18C2 0BCE391E DAE2FE4C 5810F576
Fingerprint SHA1: B7735A2E 3A5C274F C311D7F1 3BE89942 355102DE
State:
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: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
```

```
State:
Keys generated ............ Yes (General Purpose)
Issuing CA authenticated ....... Yes
Certificate request(s) ..... None

Trustpoint srstcaserver:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
State:
Keys generated ............ Yes (General Purpose)
Issuing CA authenticated ....... Yes
Certificate request(s) ..... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
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(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(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
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4RUFE
MkQyMB4XDTA2MDMwMTIxMjc1MloXDTIxMDIyNTIxMjc1MVowQTELMAkGA1UEBhMC
VVMxGjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRYwFAYDVQQDEw1DQVBGLTU4
RUFEMkQyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC99KgZT94qhozw4bOB
f8Z0tYwT2l4L++mC64O3s3AshDi8xe8Y8sN/f/ZKRRhNIxBlK4SWafXnHKJBqKZn
WtSgkRjJ3Dh0XtqcWYt8VS2sC69g8sX09lskKl3m+TpWsr2T/mDXv6CceaKN+mch
gcrrnNo8kamOOIG8OsQc4L6XzQIDAQABozEwLzAOBgNVHQ8BAf8EBAMCAoQwHQYD
quit
Certificate has the following attributes:
Fingerprint MD5: 1951DJ4E 76D79FEB FFB061C6 233C8E33
Fingerprint SHA1: 222891BE Z7B89B94 447AB8F2 5831D2AB 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(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# 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
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEdHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZXmeHjqEgVO3UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxwlANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrcxb0UH7IQJ1ogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
quit
Certificate has the following attributes:
Fingerprint MD5: 21956CBR 4B9706DF 0F3BA6B7 7P54AZ72
Fingerprint SHA1: A9917775 F86BB37A 7H130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoManufactureCA
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
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
MIIE2TCCA8GgAwIBAgIKamlnswAAAAAAAzANBgkqhkiG9w0BAQUFADA1MRYwFAYD
D/g2qgfEMkHFp68dGf/2c5k5WnNnYhM0DR9elXBSZBcG7FNcXNtq6jUAQQIBA6OC
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFNDFIiarT0Zg7K4F
kcfcWtGwR/dsMAsGA1UdDwQEAwIBhjAQBgkrBgEEAYI3FQEEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBiAEMAQTAfBgNVHSMEGDAWgBQn88gVHm6aAgkWrSugiWBf
2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1
cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9j
cmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
I+ii6itvaSN6go4cTAnPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOfTC9Fovo4ipUsG4eakqjN9GnW6JvNwxmEApcN5JlunGdGTjaubEBEpH6GC/f08
S25l3JNFBemvM2tnIwcGhiLa69yHz1khQhrpz3B1iOAkPV19TpY4gJfVb/Cbcdi6
YBmlsGGGrd1lZva5J6LuL2GbuqEwYf2+rDUU+bgtlwavw+9tzD0865XpgdOKXrbO
+nmka9eiV2TEP0zJ2+iC7AFm1BCIolblPFft6QKoSJFjB6thJksaE5/k3Npf
quit
Certificate has the following attributes:
Fingerprint MD5: 0F3BA6B7 4B9636DF 5F54BE72 24762SBR
Fingerprint SHA1: L92BB37A S9919925 5C130ED2 3E528UP8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoRootCA2048
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoRootCA2048

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
quit
Certificate has the following attributes:
Fingerprint MD5: 2G3LZ6B7 2R1995ER 6KE4WE72 3E528BB8
Fingerprint SHA1: M9912245 5C130ED2 24762JBC 3E528VF8 956E8S5H
% Do you 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 177 (required)
- Configuring SRST Fallback on Cisco Unified Communications Manager, page 178 (required)
- Configuring CAPF on Cisco Unified Communications Manager, page 180 (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. Cisco Unified Communications Manager connects to the Cisco Unified SRST Router for its device certificate. To enable credentials service, see the “Enabling Credentials Service on the Secure Cisco Unified SRST Router” section on page 168.

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 Communications Manager administration guides are at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

SUMMARY STEPS

1. Choose **SRST** in the Cisco Unified Communications Manager menu bar.
2. Add a new SRST reference.
3. Enter the appropriate settings in the SRST fields.
4. Click **Insert**.
5. Repeat Steps 2 to 4 for additional SRST references.

DETAILED STEPS

Step 1 In the menu bar in Cisco Unified Communications Manager, choose **CCMAdmin > System > SRST**.

Step 2 Click **Add New SRST Reference**.

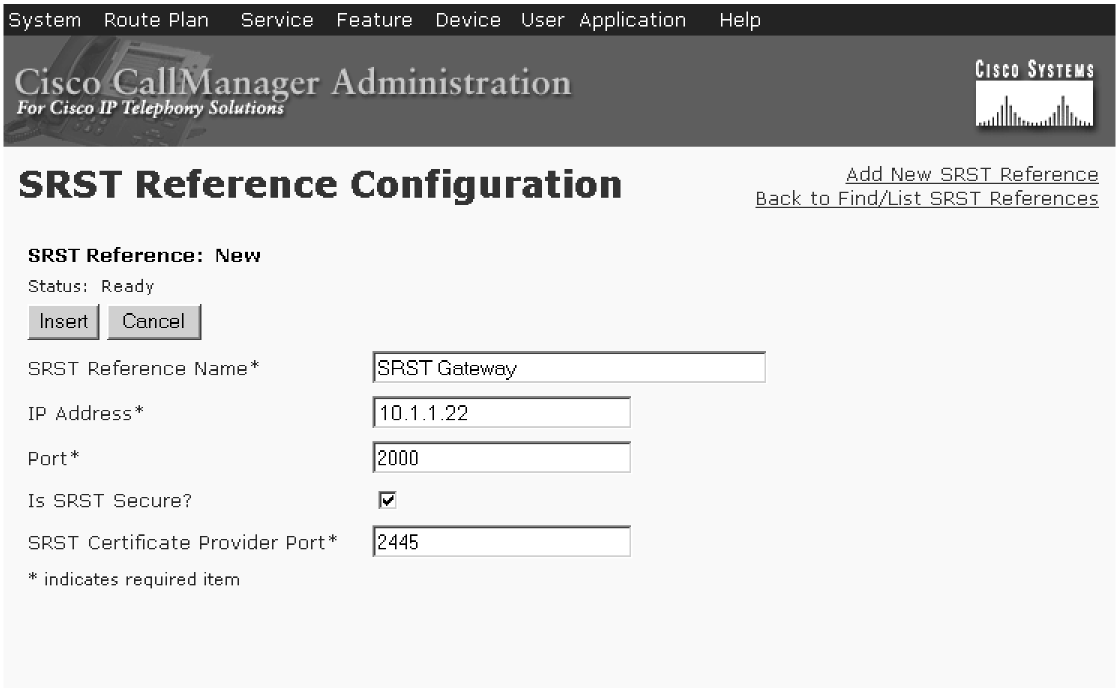
Step 3 Enter the appropriate settings. Figure 3 shows the available fields in the SRST Reference Configuration window.

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.

Figure 3 SRST Reference Configuration Window



SRST Reference Configuration

SRST Reference: New
Status: Ready

SRST Reference Name* SRST Gateway
IP Address* 10.1.1.22
Port* 2000
Is SRST Secure? ☑
SRST Certificate Provider Port* 2445
* indicates required item

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 through 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 device pool to SRST.

For complete information about adding a device pool to Cisco Unified Communications Manager, see the “Device Pool Configuration” section in the *Cisco Unified Communications Manager Administration Guide* for the Cisco Unified Communications Manager version that you are running. All Cisco Unified Communications Manager administration guides are at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

SUMMARY STEPS

1. Choose **Device Pool** in the Cisco Unified Communications Manager menu bar.
2. Add a device pool.
3. Click **Add New Device Pool.**
4. Enter the SRST reference.
5. Click **Update**.

DETAILED STEPS

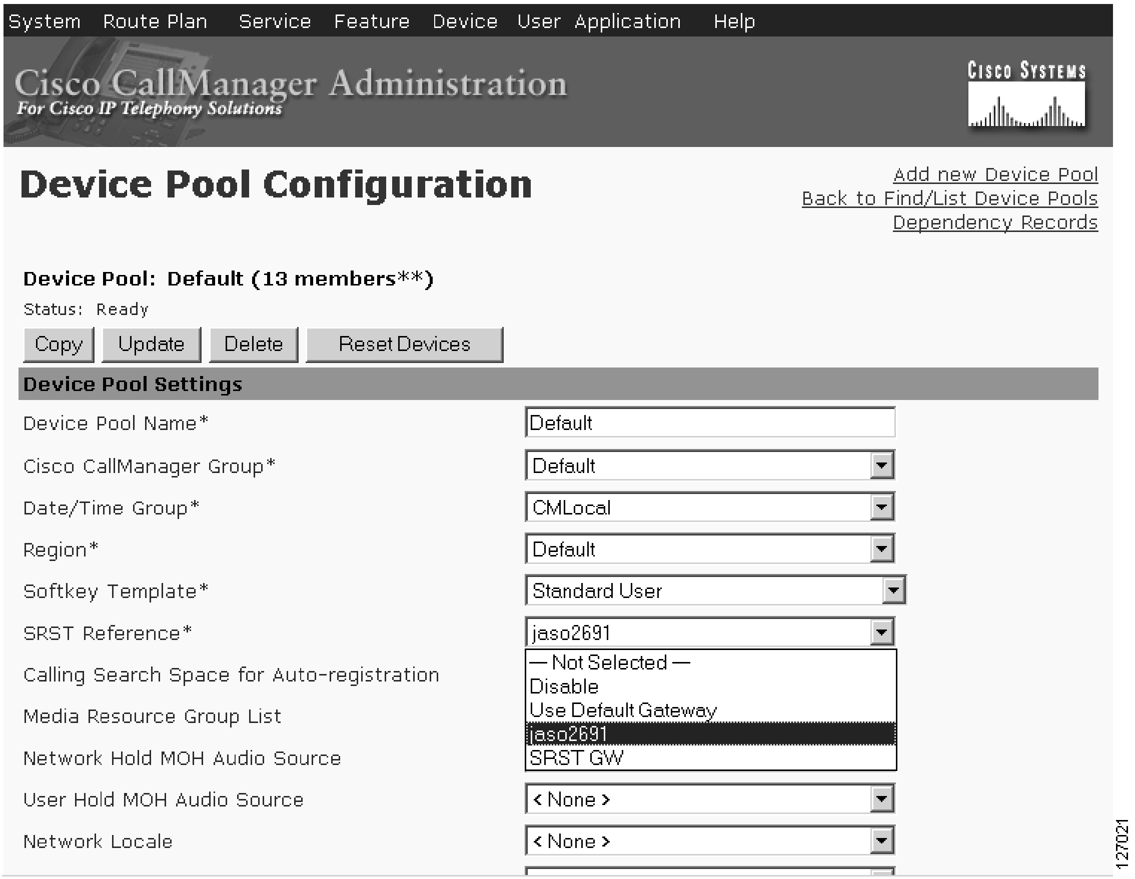
Step 1 In the menu bar in Cisco Unified Communications Manager, choose **CCMAdmin > System** > **Device Pool**.

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 4).

Figure 4 Device Pool Configuration Window



Device Pool Configuration

Device Pool: Default (13 members**)

Status: Ready

Device Pool Settings

Device Pool Name*	Default
Cisco CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	Default
Softkey Template*	Standard User
SRST Reference*	jaso2691
Calling Search Space for Auto-registration	— Not Selected — Disable Use Default Gateway jaso2691 SRST GW
Media Resource Group List	
Network Hold MOH Audio Source	
User Hold MOH Audio Source	< None >
Network Locale	< 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 Communications Manager, to request LSC certificates from Cisco Unified IP Phones. 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

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`secondary-dialtone`** *`digit-string`*
	Example:
	`Router(config-cm-fallback)# secondary-dialtone 9`
		Activates a secondary dial tone when a digit string is dialed.

Step 3	**`transfer-system`** {**`blind`** | **`full-blind`** | **`full-consult`** | **`local-consult`**}
	Example:
	`Router(config-cm-fallback)# transfer-system full-consult`
		Defines the call-transfer method for all lines served by the Cisco Unified SRST Router.
		• **blind**: Calls are transferred without consultation with a single phone line using the Cisco proprietary method.
		• **full-blind**: Calls are transferred without consultation using H.450.2 standard methods.
		• **full-consult**: Calls are transferred with consultation using a second phone line if available. The calls fallback to **full-blind** if the second line is unavailable.
		• **local-consult**:: Calls are transferred with local consultation using a second phone line if available. The calls fallback to **blind** for nonlocal consultation or nonlocal transfer target.

Step 4	**`ip source-address`** *`ip-address`* [**`port`** *`port`*] **Example:** `Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000`	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.

	Command or Action	Purpose
Step 5	**max-ephones** *max-phones* **Example:** `Router(config-cm-fallback)# max-ephones 15`	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 39 for further details.
Step 6	**max-dn** *max-directory-numbers* **Example:** `Router(config-cm-fallback)# max-dn 30`	Sets the maximum number of directory numbers (DNs) or virtual voice ports that can be supported by the router. • *max-directory-numbers:* 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 39 for further details.
Step 7	**transfer-pattern** *transfer-pattern* **Example:** `Router(config-cm-fallback)# transfer-pattern .....`	Allows transfer of telephone calls by Cisco Unified IP Phones to specified phone number patterns. • *transfer-pattern*: String of digits for permitted call transfers. Wildcards are allowed.
Step 8	**exit** **Example:** `Router(config-cm-fallback)# exit`	Exits call-manager-fallback configuration mode.

Examples

The following example enables SRST mode on your router.

```
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
```

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.

SUMMARY STEPS

1. **show ephone**
2. **show ephone offhook**
3. **show voice call status**
4. **debug ephone register**

5. **debug ephone state**

DETAILED STEPS

Step 1 **show ephone**

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 SRST. In this example, authentication and encryption status is active with a TLS connection.

```
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.

```
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
: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 49468 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
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
```

Step 3 **show voice call status**

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.

```
Router# show voice call status

CallID CID ccVdb Port DSP/Ch Called # Codec Dial-peers
0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw 20035/20027
0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw 20027/20035
0x1166 2C01 0x861043D8 50/0/21.0 2012 g711ulaw 20021/20011
0x1168 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw 20011/20021
0x1167 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw 20022/20014
0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw 20014/20022
0x116A 2C07 0x860A374C 50/0/12.0 2010 g711ulaw 20012/20002
0x116B 2C07 0x86039700 50/0/2.0 *2010 g711ulaw 20002/20012
0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020
0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023
0x116E 2C0D 0x8608DC20 50/0/10.0 2022 g711ulaw 20010/20008
0x116F 2C0D 0x86078AD8 50/0/8.0 *2022 g711ulaw 20008/20010
0x1170 2C10 0x861398F0 50/0/26.0 2016 g711ulaw 20026/20028
0x1171 2C10 0x8614F41C 50/0/28.0 *2016 g711ulaw 20028/20026
0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw 20029/20004
0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw 20004/20029
0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw 20025/20030
0x1175 2C16 0x86164F48 50/0/30.0 *2026 g711ulaw 20030/20025
0x1176 2C19 0x860D8C64 50/0/17.0 2032 g711ulaw 20017/20018
0x1177 2C19 0x860E4008 50/0/18.0 *2032 g711ulaw 20018/20017
0x1178 2C1C 0x860CE3C0 50/0/16.0 2004 g711ulaw 20016/20019
0x1179 2C1C 0x860EE8AC 50/0/19.0 *2004 g711ulaw 20019/20016
0x117A 2C1F 0x86043FA4 50/0/3.0 2008 g711ulaw 20003/20024
0x117B 2C1F 0x861247A8 50/0/24.0 *2008 g711ulaw 20024/20003
0x117C 2C22 0x8608337C 50/0/9.0 2020 g711ulaw 20009/20031
0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw 20031/20009
0x117E 2C25 0x86063990 50/0/6.0 2006 g711ulaw 20006/20001
0x117F 2C25 0x85C6BE6C 50/0/1.0 *2006 g711ulaw 20001/20006
0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20013/20034
0x1181 2C28 0x8618FBBC 50/0/34.0 *2029 g711ulaw 20034/20013
0x1182 2C2B 0x860C3B1C 50/0/15.0 2036 g711ulaw 20015/20005
0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20015
0x1184 2C2E 0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007
0x1185 2C2E 0x8606E234 50/0/7.0 *2024 g711ulaw 20007/20032
0x1186 2C31 0x861A56E8 50/0/36.0 2030 g711ulaw 20036/20033
0x1187 2C31 0x86185318 50/0/33.0 *2030 g711ulaw 20033/20036
18 active calls found
```

Step 4 **debug ephone register**

Use this command to debug the process of Cisco IP phone registration.

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
```

Step 5 **debug ephone state**

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.

```
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]:OFFHOOK
*Jan 11 18:33:11.747:ephone-2[2]:---SkinnySyncPhoneDnOverlays 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:DtInsideDialTone onoff=1 
pid=232
*Jan 11 18:33:15.031:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence 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]::callingParty 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 18:33:16.039:ephone-2[2]:6001
*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]::callingParty 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
*Jan 11 18:33:16.047:ephone-3[3]:Ringer Inside Ring On
*Jan 11 18:33:16.051:dn_tone_control DN=2 chan 1 tonetype=36:DtAlertingTone onoff=1 
pid=232
*Jan 11 18:33:20.831:ephone-3[3]:OFFHOOK
*Jan 11 18:33:20.831:ephone-3[3]:---SkinnySyncPhoneDnOverlays is onhook
*Jan 11 18:33:20.831:ephone-3[3]:Ringer Off
*Jan 11 18:33:20.831:ephone-3[3]:ANSWER call
*Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsOffHook
*Jan 11 18:33:20.831:ephone-3[3][SEP000DEDAB3EBF]:Answer Incoming call from ephone-(2) DN 
2 chan 1
*Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsConnected
*Jan 11 18:33:20.831:defer_start for DN 2 chan 1 at CONNECTED
```

```
*Jan 11 18:33:20.831:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsConnected
*Jan 11 18:33:20.835:ephone-3[3]::callingNumber 6000

*Jan 11 18:33:20.835:ephone-3[3]::callingParty 6000

*Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 4 called 6001
calling 6000 origcalled
*Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000
origcalled 6001 calltype 1
*Jan 11 18:33:20.835:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:20.835:ephone-3[3]:Original Called Name 6001
*Jan 11 18:33:20.835:ephone-3[3]:6000 calling
*Jan 11 18:33:20.835:ephone-3[3]:6001
*Jan 11 18:33:20.835:ephone-2[2]:Security Key Generation
! Ephone 2 generates a security key.

*Jan 11 18:33:20.835:ephone-2[2]:OpenReceive DN 2 chan 1 codec 4:G711Ulaw64k  duration 20
ms bytes 160
*Jan 11 18:33:20.835:ephone-2[2]:Send Decryption Key
! Ephone 2 sends the decryption key.

*Jan 11 18:33:20.835:ephone-3[3]:Security Key Generation
!Ephone 3 generates its security key.

*Jan 11 18:33:20.835:ephone-3[3]:OpenReceive DN 4 chan 1 codec 4:G711Ulaw64k  duration 20
ms bytes 160
*Jan 11 18:33:20.835:ephone-3[3]:Send Decryption Key
! Ephone 3 sends its decryption key.

*Jan 11 18:33:21.087:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232
*Jan 11 18:33:21.087:DN 4 chan 1 Voice_Mode
*Jan 11 18:33:21.091:DN 2 chan 1 End Voice_Mode
*Jan 11 18:33:21.091:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:21.095:ephone-2[2]:OpenReceiveChannelAck:IP 1.1.1.8, port=25552,
               dn_index=2, dn=2, chan=1
*Jan 11 18:33:21.095:ephone-3[3]:StartMedia 1.1.1.8 port=25552
*Jan 11 18:33:21.095:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160
*Jan 11 18:33:21.095:ephone-3[3]:Send Encryption Key
! Ephone 3 sends its encryption key.

*Jan 11 18:33:21.347:ephone-3[3]:OpenReceiveChannelAck:IP 1.1.1.9, port=17520,
               dn_index=4, dn=4, chan=1
*Jan 11 18:33:21.347:ephone-2[2]:StartMedia 1.1.1.9 port=17520
*Jan 11 18:33:21.347:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160
*Jan 11 18:33:21.347:ephone-2[2]:Send Encryption Key
!Ephone 2 sends its encryption key.*Jan 11 18:33:21.851:ephone-2[2]::callingNumber 6000

*Jan 11 18:33:21.851:ephone-2[2]::callingParty 6000
*Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 4 called 6001
calling 6000 origcalled
*Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000
origcalled 6001 calltype 2
*Jan 11 18:33:21.851:ephone-2[2]:Call Info for chan 1
*Jan 11 18:33:21.851:ephone-2[2]:Original Called Name 6001
*Jan 11 18:33:21.851:ephone-2[2]:6000 calling
*Jan 11 18:33:21.851:ephone-2[2]:6001
```

Configuration Examples for Secure SRST

This section provides the following configuration examples.

- Secure SRST: Example, page 187
- Control Plane Policing: Example, page 192

Note IP addresses and hostnames in examples are fictitious.

Secure 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
!
! Define root CA.
crypto pki server srstcaserver
 database level complete
 database url nvram
 issuer-name CN=srstcaserver

!
crypto pki trustpoint srstca
 enrollment url http://10.1.1.22:80
 revocation-check none
!
crypto pki trustpoint srstcaserver
 revocation-check none
 rsakeypair srstcaserver
!
! Define CTL/7970 trustpoint.
crypto pki trustpoint 7970
 enrollment terminal
 revocation-check none
!
crypto pki trustpoint PEM
 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 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 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
  32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
  C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
  FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
  03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
  06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
  CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
  FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
  B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
  C3AF4A66 BD007348 D013000A EA3C206D CF
  quit
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
  55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
  1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
  9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
  47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
  C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
  DEDBAAD7 3780136E B112A6
  quit
crypto pki certificate chain srstcaserver
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
  55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
  1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
  9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
  47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
  C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
  DEDBAAD7 3780136E B112A6
  quit
crypto pki certificate chain 7970
 certificate ca 353FB24BD70F14A346C1F3A9AC725675
  308203A8 30820290 A0030201 02021035 3FB24BD7 0F14A346 C1F3A9AC 72567530
  0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
  20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3032301E
  170D3033 31303130 32303138 34395A17 0D323331 30313032 30323733 375A302E
  31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
  03130B43 41502D52 54502D30 30323082 0120300D 06092A86 4886F70D 01010105
  00038201 0D003082 01080282 010100C4 266504AD 7DC3FD8D 65556FA6 308FAE95
  B570263B 575ABD96 1CC8F394 5965D9D0 D8CE02B9 F808CCD6 B7CD8C46 24801878
  57DC4440 A7301DDF E40FB1EF 136212EC C4F3B50F BCAFBB4B CD2E5826 34521B65
  01555FE4 D4206776 03368357 83932638 D6FC953F 3A179E44 67255A73 45C69DEE
  FB4D221B 21D7A3AD 38184171 8FD8C271 42183E65 09461434 736C77CC F380EEBF
  632C7B3F A5F92AA6 A8EF3490 8724A84F 4DAF7FD7 0928F585 764D3558 3C0FE9AF
  1ED8763F A299A802 970004AD 1912D265 7DE335B4 BCB6F789 DC68B9FA C8FDF85E
  8A28AD8F 0F4883C0 77112A47 141DBEE0 948FBE53 FE67B308 D40C8029 87BD790E
  CDAB9FD7 A190C1A2 A462C5F2 4A6E0B02 0103A381 C33081C0 300B0603 551D0F04
  04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  1452922B E288EE2E 098A4E7E 702C56A5 9AB4D49B 96306F06 03551D1F 04683066
  3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30322F43 65727445
  6E726F6C 6C2F4341 502D5254 502D3030 322E6372 6C862F66 696C653A 2F2F5C5C
  6361702D 7274702D 3030325C 43657274 456E726F 6C6C5C43 41502D52 54502D30
  30322E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
  F70D0101 05050003 82010100 56838CEF C4DA3AD1 EA8FBB15 2FFE6EE5 50A1972B
  D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D DC0C4B92 5AA94B6E 69277F9B
  FC73C697 11266E19 451C0FAB A55E6A28 901A48C5 B9911EE6 348A8920 0AEDE1E0
  B6EA781C FFD97CA4 B03C0E34 0E5B0649 8B0A34C9 B73A654E 09050C1F 4DA53E44
  BF78443D B08C3A41 2EEEB873 78CB8089 34F9D16E 91512F0D 3A8674AD 0991ED1A
  92841E76 36D7740E CB787F11 685B9E9D 0C67E85D AF6D05BA 3488E86D 7E2F7F65
  6918DE0F BD3C7F67 D8A33F70 9C4A596E D9F62B3B 1EDEE854 D5882AD4 3D71F72B
  8FAB7F3C 0B5F0759 D9828F83 954D7BB1 57A638EC 7D72BFF1 8933C16F 760BCA94
  4C5B1931 67947A4F 89A1BDB5
  quit
crypto pki certificate chain PEM
 certificate ca 7612F960153D6F9F4E42202032B72356
  308203A8 30820290 A0030201 02021076 12F96015 3D6F9F4E 42202032 B7235630
  0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
  20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3031301E
  170D3033 30323036 32333237 31335A17 0D323330 32303632 33333633 345A302E
  31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
  03130B43 41502D52 54502D30 30313082 0120300D 06092A86 4886F70D 01010105
  00038201 0D003082 01080282 010100AC 55BBED18 DE9B8709 FFBC8F2D 509AB83A
  21C1967F DEA7F4B0 969694B7 80CC196A 463DA516 54A28F47 5D903B5F 104A3D54
  A981389B 2FC7AC49 956262B8 1C143038 5345BB2E 273FA7A6 46860573 CE5C998D
  55DE78AA 5A5CFE14 037D695B AC816409 C6211F0B 3BBF09CF B0BBB2D4 AC362F67
  0FD145F1 620852B3 1F07E2F1 AA74F150 367632ED A289E374 AF0C5B78 CE7DFB9F
  C8EBBE54 6ECF4C77 99D6DC04 47476C0F 36E58A3B 6BCB24D7 6B6C84C2 7F61D326
  BE7CB4A6 60CD6579 9E1E3A84 8153B750 5527E865 423BE2B5 CB575453 5AA96093
  58B6A2E4 AA3EF081 C7068EC1 DD1EBDDA 53E6F0D6 E2E0486B 109F1316 78C696A3
  CFBA84CC 7094034F C1EB9F81 931ACB02 0103A381 C33081C0 300B0603 551D0F04
  04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E917B1 82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06 03551D1F 04683066
  3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30312F43 65727445
  6E726F6C 6C2F4341 502D5254 502D3030 312E6372 6C862F66 696C653A 2F2F5C5C
  6361702D 7274702D 3030315C 43657274 456E726F 6C6C5C43 41502D52 54502D30
  30312E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
  F70D0101 05050003 82010100 AB64FDEB F60C32DC 360F0E10 5FE175FA 0D574AB5
  02ACDCA3 C7BBED15 A4431F20 7E9286F0 770929A2 17E4CDF4 F2629244 2F3575AF
  E90C468C AE67BA08 AAA71C12 BA0C0E79 E6780A5C F814466C 326A4B56 73938380
  73A11AED F9B9DE74 1195C48F 99454B8C 30732980 CD6E7123 8B3A6D68 80B97E00
  7F4BD4BA 0B5AB462 94D9167E 6D8D48F2 597CDE61 25CFADCC 5BD141FB 210275A2
  0A4E3400 1428BA0F 69953BB5 50D21F78 43E3E563 98BCB2B1 A2D4864B 0616BACD
  A61CD9AE C5558A52 B5EEAA6A 08F96528 B1804B87 D26E4AEE AB7AFFE9 2FD2A574
  BAFE0028 96304A8B 13FB656D 8FC60094 D5A53D71 444B3CEF 79343385 3778C193
  74A2A6CE DC56275C A20A303D
  quit
crypto pki certificate chain 7960
 certificate ca F301
  308201F7 30820160 A0030201 020202F3 01300D06 092A8648 86F70D01 01050500
  3041310B 30090603 55040613 02555331 1A301806 0355040A 13114369 73636F20
  53797374 656D7320 496E6331 16301406 03550403 130D4341 50462D33 35453038
  33333230 1E170D30 34303430 39323035 3530325A 170D3139 30343036 32303535
  30315A30 41310B30 09060355 04061302 5553311A 30180603 55040A13 11436973
  636F2053 79737465 6D732049 6E633116 30140603 55040313 0D434150 462D3335
  45303833 33323081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
  818100C8 BD9B6035 366B44E8 0F693A47 250FF865 D76C35F7 89B1C4FD 1D122CE0
  F5E5CDFF A4A87EFF 41AD936F E5C93163 3E55D11A AF82A5F6 D563E21C EB89EBFA
  F5271423 C3E875DC E0E07967 6E1AAB4F D3823E12 53547480 23BA1A09 295179B6
  85A0E83A 77DD0633 B9710A88 0890CD4D DB55ADD0 964369BA 489043BB B667E60F
  93954B02 03010001 300D0609 2A864886 F70D0101 05050003 81810056 60FD3AB3
  6F98D2AD 40C309E2 C05B841C 5189271F 01D864E8 98BCE665 2AFBCC8C 54007A84
  8F772C67 E3047A6C C62F6508 B36A6174 B68C1D78 C2228FEA A89ECEFB CC8BA9FC
  0F30E151 431670F9 918514D9 868D1235 18137F1E 50DFD32E 1DC29CB7 95EF4096
  421AF22F 5C1D5804 B83F8E8E 95B04F45 86563BFE DF976C5B FB490A
  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
 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
.
.
.
```

Where to Go Next

If you require voice mail, see the voice-mail configuration instructions in the “Integrating Voice Mail with Cisco Unified SRST” section on page 193. You may also want to read the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Integrating Voice Mail with Cisco Unified SRST

Revised: July 11, 2008
This chapter describes how to make your existing voice-mail system run on phones connected to a Cisco Unified (SRST) router during Cisco Unified Communications Manager fallback.

Contents

Information About Integrating Voice Mail with Cisco Unified SRST

Cisco Unified SRST can send and receive voice-mail messages from Cisco Unity and other voice-mail systems during Cisco Unified Communications Manager fallback. When the WAN is down, a voice-mail system with BRI or PRI access to the Cisco Unified SRST system uses ISDN signaling (see Figure 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 2).

Figure 1 Cisco Unified Communications Manager Fallback with BRI or PRI

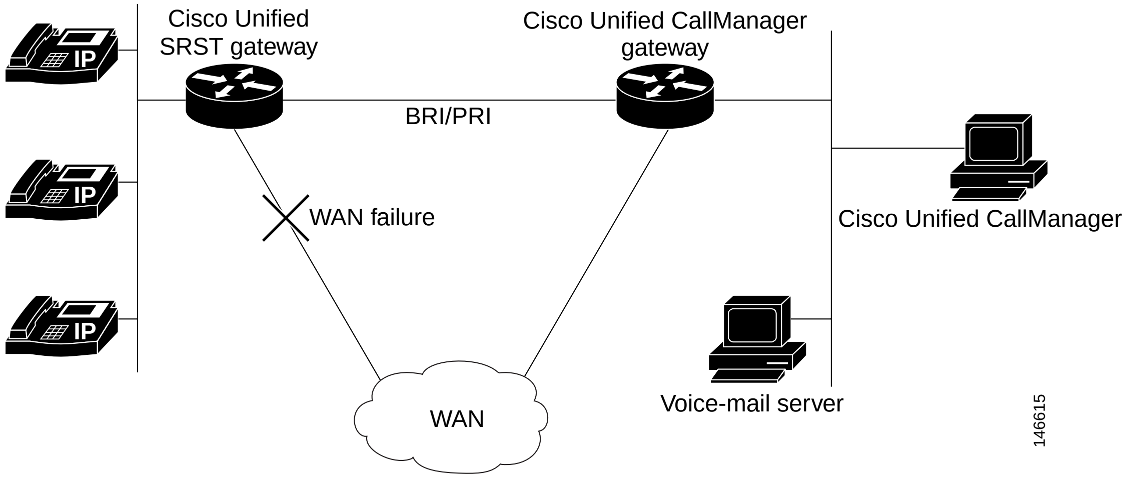
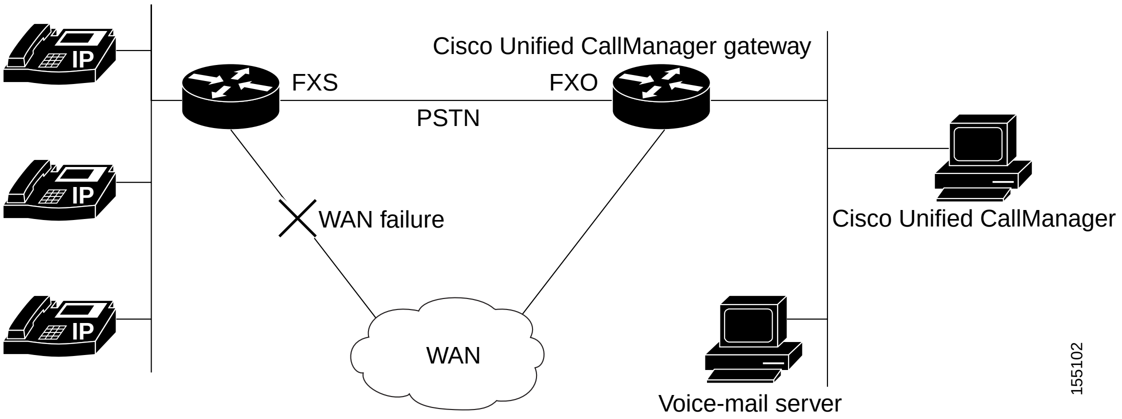

Cisco Unified SRST gateway
Cisco Unified CallManager gateway
BRI/PRI
WAN failure
Cisco Unified CallManager
Voice-mail server
WAN
146615

Figure 2 Cisco Unified Communications Manager Fallback with PSTN



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 voice-mail system. To make this happen, you must configure access from the dial peers to the voice-mail system and establish routing to the voice-mail system for busy and unanswered calls and for message buttons.

If the voice-mail system is accessed over FXO or FXS, you must configure instructions (DTMF patterns) for the voice-mail system so that it can access the correct voice-mail system mailbox. If your voice-mail system is accessed over BRI or PRI, no instructions are necessary because the voice-mail system can log in to the calling phone's mailbox directly.

How to Integrate Voice Mail with Cisco Unified SRST

This section contains the following tasks:

- Configuring Direct Access to Voice Mail, page 195 (Required)
- Configuring Message Buttons, page 198 (Required)
- Redirecting to Cisco Unified Communications Manager Gateway, page 200 (Required for BRI or PRI))
- Configuring Call Forwarding to Voice Mail, page 200 (Required FXO or FXS)
- Configuring Message Waiting Indication, page 204 (Optional)

Configuring Direct Access to Voice Mail

To access voice-mail messages with FXO or FXS access, you must have POTS dial peers configured with a destination pattern that matches the voice-mail system's number. Also, you must associate the dial peer with the port to which the voice-mail system is accessed.

Both sets of configurations are done in global configuration mode and 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

	Command or Action	Purpose

Step 1	`dial-peer voice` *tag* {**pots** | **voatm** | **vofr** | **voip**}
	Example:
	`Router(config)#` **`dial-peer voice 1002 pots`**
		(FXO or FXS and BRI or PRI) Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial-peer configuration mode. The **dial-peer** command provides different syntax for individual routers. This example is syntax for Cisco 3600 series routers.
		• *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	**`destination-pattern`** [**+**] *string* [**T**] **Example:** `Router(config-dial-peer)# destination-pattern 1100T`	(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. • **+**: (Optional) Character that indicates an E.164 standard number. • *string*: See Table 1. • **T**: (Optional) Control character that indicates that the destination-pattern value is a variable-length dial string.

Step 3	**`port`** {*slot-number*/*subunit-number*/*port* | *slot*/*port*:*ds0-group-no*}
	Example:
	`Router(config-dial-peer)# port 1/1/1`
		(FXO or FXS and BRI or PRI) Associates a dial peer with a specific voice port on Cisco 3600 series routers.
		• *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.

	Command or Action	Purpose

Step 4	`forward-digits {num-digit | all | extra}`
	Example:
	`Router(config-dial-peer)# forward-digits all`
		(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.

Step 5	`exit`
	Example:
	`Router(config-dial-peer)# exit`
		(FXO or FXS and BRI or PRI) Exits dial-peer configuration mode.

Table 1 Valid Entries for the string Argument in the destination-pattern command

Entry	Description
Digits 0 to 9	—
Letters A through D	—
Asterisk (*) and pound sign (#)	These appear on standard touch-tone dial pads.
Comma (,)	Inserts a pause between digits.
Period (.)	Matches any entered digit (this character is used as a wildcard).
Percent sign (%)	Indicates that the preceding digit occurred zero or more times; similar to the wildcard usage.
Plus sign (+)	Indicates that the preceding digit occurred one or more times. **Note** 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.
Circumflex (^)	Indicates a match to the beginning of the string. Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
Dollar sign ($)	Matches the null string at the end of the input string.
Backslash symbol (\)	Is followed by a single character and matches that character. Can be used with a single character with no other significance (matching that character).
Question mark (?)	Indicates that the preceding digit occurred zero or one time.
Brackets ([ ])	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.

Examples

The following FXO and FXS example sets up a POTS dial peer named 1102, matches dial-peer 1102 to voice-mail extension 1101, and assigns dial-peer 1102 to voice-port 1/1/1 where the voice-mail system is connected. Other dial peers are configured for direct access to voice mail.

```
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.

```
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 SRST router during Cisco Unified Unified Communications Manager fallback, you must program a speed-dial number to the voice-mail system. The speed-dial number is dialed when message buttons on phones connected to the Cisco Unified SRST router are pressed during Cisco Unified Communications Manager fallback. In addition, call forwarding must be configured so that calls to busy and unanswered numbers are sent to the voice-mail 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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`voicemail`** *`phone-number`*
	Example:
	`Router(config-cm-fallback)#` **`voicemail 5550100`**
		Configures the telephone number that is dialed when the message button on a Cisco Unified IP Phone is pressed.
		• *phone-number*: Phone number configured as a speed-dial number for retrieving messages.

Step 3	**`call-forward busy`** *`directory-number`*
	Example:
	`Router(config-cm-fallback)# call-forward busy 2000`
		Configures call forwarding to another number when the Cisco IP phone is busy.
		• *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.

Step 4	**`call-forward noan`** *`directory-number`* **`timeout`** *`seconds`*
	Example:
	`Router(config-cm-fallback)# call-forward noan 2000 timeout 10`
		Configures call forwarding to another number when no answer is received from the Cisco IP phone.
		• *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.
		• **timeout** *seconds*: Sets the waiting time, in seconds, before the call is forwarded to another phone. The *seconds* range is from 3 to 60000.

Step 5	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

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 voice-mail number (1101).

```
call-manager-fallback
 voicemail 1101
 call-forward busy 1101
 call-forward noan 1101 timeout 3
```

Redirecting to Cisco Unified Communications Manager Gateway

Note The following task is required for voice-mail 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 voice-mail systems. Voice-mail systems with BRI or PRI access can log in to the calling phone's mailbox directly. For this to happen, some Cisco Unified Communications Manager configuration is recommended. If your voice-mail system supports Redirected Dialed Number Identification Service (RDNIS), RDNIS must be included in the outgoing SETUP message to Cisco Unified Communications Manager 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 Communications Manager, 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 Voice Mail

Note The following task is required for voice-mail 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 voice-mail systems. The forwarded calls can be routed to almost any location in the voice-mail system. Typically, calls are forwarded to a location in the called number's mailbox where the caller can leave messages.

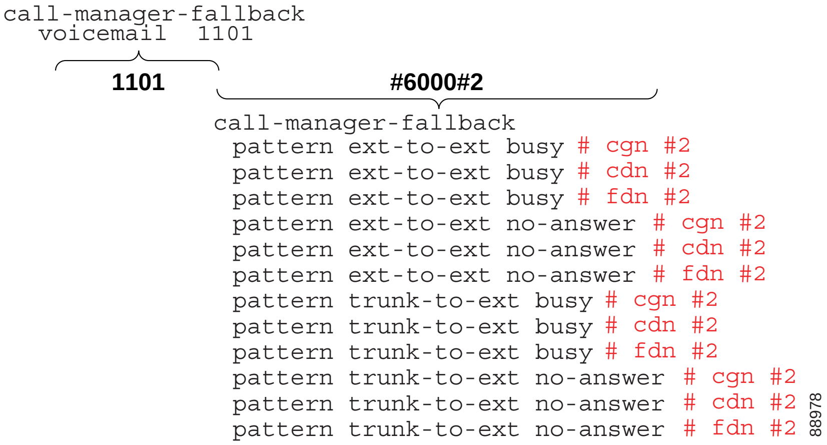
Call Routing Instructions Using DTMF Digit Patterns

Cisco Unified SRST call-routing instructions are required so that forwarded calls can be sent to the correct voice mailboxes. These instructions consist of DTMF digits configured in patterns that match the dial sequences required by the voice-mail system to get to a particular voice-mail location. For example, a voice-mail system may be designed so that callers must do the following to leave a message:

1. Dial the central voice-mail 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 3, this is accomplished through the **voicemail** and **pattern** commands.

Figure 3 How Voice-Mail Dial Sequence 1101#6000#2 Is Configured in Cisco Unified SRST



```
call-manager-fallback
  voicemail  1101
```

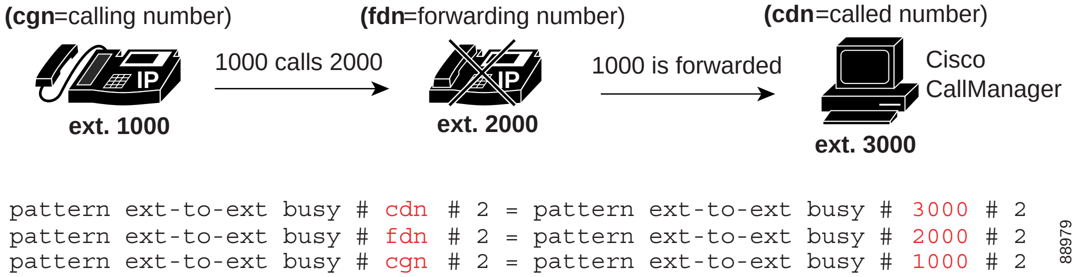
```
call-manager-fallback
 pattern ext-to-ext busy # cgn #2
 pattern ext-to-ext busy # cdn #2
 pattern ext-to-ext busy # fdn #2
 pattern ext-to-ext no-answer # cgn #2
 pattern ext-to-ext no-answer # cdn #2
 pattern ext-to-ext no-answer # fdn #2
 pattern trunk-to-ext busy # cgn #2
 pattern trunk-to-ext busy # cdn #2
 pattern trunk-to-ext busy # fdn #2
 pattern trunk-to-ext no-answer # cgn #2
 pattern trunk-to-ext no-answer # cdn #2
 pattern trunk-to-ext no-answer # fdn #2
```

The # cgn #2, # cdn #2, and # fdn #2 portions of the **pattern** commands shown in Figure 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 voice mail.

A tag can be up to three character from the DTMF tone set (A to D, 0 to 9, # and *). Voice-mail 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 voice-mail system.

Tokens tell Cisco Unified SRST what telephone number in the call forwarding chain to use in the pattern. As shown in Figure 4, there are three types of tokens that correspond to three possible call states during voice-mail forwarding.

Figure 4 How Numbers Are Extracted from Tokens



```
pattern ext-to-ext busy # cdn # 2 = pattern ext-to-ext busy # 3000 # 2
pattern ext-to-ext busy # fdn # 2 = pattern ext-to-ext busy # 2000 # 2
pattern ext-to-ext busy # cgn # 2 = pattern ext-to-ext busy # 1000 # 2
```

Sets of tags and tokens or patterns activate a voice-mail system when

- 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 voice mail (**pattern ext-to-ext busy** command).
- An internal extension fails to connect to an extension and the call is forwarded to voice mail (**pattern ext-to-ext no-answer** command).
- An external trunk call reaches a busy extension and the call is forwarded to voice mail (**pattern trunk-to-ext busy** command).
- An external trunk call reaches an unanswered extension and the call is forwarded to voice mail (**pattern trunk-to-ext no-answer** command).

Prerequisites

- FXO hairpin-forwarded calls to voice-mail 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 voice-mail system will interpret correctly, you must know how the system routes voice-mail calls and interprets DTMF tones (see the “Call Routing Instructions Using DTMF Digit Patterns” section on page 201).

  You can find information about how Cisco Unity handles voice-mail 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 voice-mail systems, see the analog voice mail 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-tag*]
3. **pattern ext-to-ext busy** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]
4. **pattern ext-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]
5. **pattern trunk-to-ext busy** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]

6. **pattern trunk-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`vm-integration`**
	Example:
	`Router(config)# vm-integration`
		Enters voice-mail integration mode and enables voice-mail integration with DTMF and analog voice-mail systems.

Step 2	**pattern direct** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-int)# pattern direct 2 CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when the user presses the messages button on the phone. • *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 voice-mail 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 voice-mail system. • **CDN**: Called number (CDN) information is sent to the voice-mail system. • **FDN**: Forwarding number (FDN) information is sent to the voice-mail system.
Step 3	**pattern ext-to-ext busy** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-int)# pattern ext-to-ext busy 7 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an internal extension attempts to connect to a busy extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.
Step 4	**pattern ext-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-int)# pattern ext-to-ext no-answer 5 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an internal extension fails to connect to an extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.

	Command or Action	Purpose
Step 5	**pattern trunk-to-ext busy** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-int)# pattern trunk-to-ext busy 6 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an external trunk call reaches a busy extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.
Step 6	**pattern trunk-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-int)# pattern trunk-to-ext no-answer 4 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when an external trunk call reaches an unanswered extension and the call is forwarded to voice mail. For argument and keyword information, see Step 2.

Examples

For the following configuration, if the voice-mail 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.

```
vm-integration
 pattern direct * CGN
```

For the following configuration, if 3001 calls 3006 and 3006 does not answer, the SRST router will forward 3001 to the voice-mail system (1101) and send to the voice-mail 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.

```
vm-integration
 pattern ext-to-ext no-answer # FDN #2
```

For the following configuration, if 3006 is busy and 3001 calls 3006, the SRST router will forward 3001 to the voice-mail system (1101) and send to the voice-mail 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.

```
vm-integration
 pattern ext-to-ext busy # FDN #2
```

Configuring Message Waiting Indication

The MWI relay mechanism is initiated after someone leaves a voice-mail message on the remote voice-mail message system. MWI relay is required when one Cisco Unity Voice Mail system is shared by multiple Cisco Unified SRST routers. SRST routers use the SIP Subscribe and Notify methods for MWI. See the *Configuring Cisco IOS SIP Configuration Guide* for more information on SIP MWI and the Subscribe and Notify methods. The SRST router that is the SIP MWI relay server acts as the SIP notifier. The other remote routers act as the SIP subscribers.

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

	Command	Purpose

Step 1	**`call-manager-fallback`**
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 2	**`mwi relay`**
	Example:
	`Router(config-cm-fallback)# mwi relay`
		Enables the SRST router to relay MWI information to remote Cisco IP phones.

Step 3	**`mwi reg-e164`**
	Example:
	`Router(config-cm-fallback)# mwi reg-e164`
		Registers E.164 numbers rather than extension numbers with a SIP proxy or registrar.

Step 4	**`exit`**
	Example:
	`Router(config-cm-fallback)# exit`
		Exits call-manager-fallback configuration mode.

Step 5	**`sip-ua`**
	Example:
	`Router(config)# sip-ua`
		Enters SIP user-agent configuration mode.

	Command	Purpose
Step 6	**mwi-server** {**ipv4:***destination-address* | **dns:***host-name*} [**expires** *seconds*] [**port** *port*] [**transport** {**tcp** | **udp**}] [**unsolicited**] **Example:** `Router(config-sip-ua)# mwi-server ipv4:10.0.2.254`	Configures voice-mail 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 voice-mail server. The MWI server is a Cisco Unified SRST router. Keywords and arguments are as follows: • **ipv4:***destination-address*: IP address of the voice-mail server. • **dns:***host-name*: Host device housing the domain name server that resolves the name of the voice-mail server. The argument should contain the complete hostname to be associated with the target address; for example, **dns:test.cisco.com**. • **expires** *seconds*: Subscription expiration time, in seconds. Range is from 1 to 999999. Default is 3600. • **port** *port*: Port number on the voice-mail server. Default is 5060. • **transport**: Transport protocol to the voice-mail server. Valid values are tcp and udp. Default is UDP. • **unsolicited**: Requires the voice-mail server to send a SIP notification message to the voice gateway or UA if the mailbox status changes. Removes the requirement that the voice gateway subscribe for MWI service.
Step 7	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits SIP user-agent configuration mode.

Configuration Examples

This section provides the following configuration examples:

- Configuring Local Voice-Mail System (FXO and FXS): Example, page 207
- Configuring Central Location Voice-Mail System (FXO and FXS): Example, page 207
- Configuring Voice-Mail Access over FXO and FXS: Example, page 208
- Configuring Voice-Mail Access over BRI and PRI: Example, page 209

Configuring Local Voice-Mail System (FXO and FXS): Example

The “Dial-Peer Configuration for Integration of Voice-Mail with Cisco Unified SRST” section of the example below shows a legacy dial-peer configuration for a local voice-mail system. The “Cisco Unified SRST Voice-Mail Integration Pattern Configuration” section must be compatible with your voice-mail system configuration.

```
! Dial-Peer Configuration for Integration of Voice-Mail 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
 ip source-address 1.4.214.104 port 2000
 voicemail 14011
 call-forward busy 14011
 call-forward noan 14011 timeout 3

! Cisco Unified SRST Voice-Mail 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 Voice-Mail System (FXO and FXS): Example

The “Dial-Peer Configuration for Integration of Voice-Mail with Cisco Unified SRST in Central Location” section of the example shows a legacy dial-peer configuration for a central voice-mail system. The “Cisco Unified SRST Voice-Mail Integration Pattern Configuration” section must be compatible with your voice-mail system configuration.

Note Message waiting indicator (MWI) integration is not supported for PSTN access to voice-mail systems at central locations.

```
! Dial-Peer Configuration for Integration of Voice-Mail 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 Voice-Mail 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 Voice-Mail Access over FXO and FXS: Example

The following example shows how to configure the Cisco Unified SRST router to forward unanswered calls to voice mail. In this example, the voice-mail number is 1101, the voice-mail system is connected to FXS voice port 1/1/1, and the voice mailbox numbers are 3001, 3002, and 3006.

```
voice-port 1/1/1
 timing digit 250
 timing inter-digit 250

dial-peer voice 1102 pots
 destination-pattern 1101T
 port 1/1/1

call-manager-fallback
 timeouts interdigit 5
 ip source-address 1.6.0.199 port 2000
 max-ephones 24
 max-dn 24
 transfer-pattern 3...
 voicemail 1101
 call-forward busy 1101
 call-forward noan 1101 timeout 3
 moh minuet.au

vm-integration
 pattern direct * CGN
 pattern ext-to-ext no-answer # FDN #2
 pattern ext-to-ext busy # FDN #2
 pattern trunk-to-ext no-answer # FDN #2
 pattern trunk-to-ext busy # FDN #2
```

Configuring Voice-Mail Access over BRI and PRI: Example

The following example shows how to configure the Cisco Unified SRST router to forward unanswered calls to voice mail. In this example, the voice-mail number is 1101, the voice-mail 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...
 voicemail 1101
 call-forward busy 1101
 call-forward noan 1101 timeout 3
 moh minuet.au
```

Where to Go Next

For information about monitoring and maintaining Cisco Unified SRST, go to the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Setting Video Parameters

Revised: July 11, 2008

This chapter describes how to set video parameters for a Cisco Unified Survivable Remote Site Telephony (SRST) Router.

Contents

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 Communications Manager 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 the *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)

- Perform basic Cisco Unified SRST configuration. For more information, see *Cisco Unified SRST V4.0: Setting Up the Network*.
- Perform basic ephone configuration. For more information, see *Cisco Unified SRST V4.0: Setting Up Cisco Unified IP Phones*.

Restrictions for Setting Video Parameters

- This feature supports only the following video codecs:
  - H.261
  - H.263
- 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 Communications Manager. 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 Communications Manager. 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 213
- Retrieving Video Codec Information, page 213
- Call Fallback to Audio-Only, page 213
- Call Setup for Video Endpoints, page 213
- Flow of the RTP Video Stream, page 214

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 show 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 Communications Manager. 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 215
- Verifying Cisco Unified SRST, page 216
- Setting Video Parameters for Cisco Unified SRST, page 223

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**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode.

Step 4	**`h323`**
	Example:
	`Router(config-voi-serv)# h323`
		Enters H.323 voice-service configuration mode.

Step 5	**`call start slow`**
	Example:
	`Router(config-serv-h323)# call start slow`
		Forces an H.323 gateway to use slow-connect procedures for all VoIP calls.

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. s**how call-manager-fallback all**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`show running config`**
	Example:
	`Router# show running config`
		Displays the entire contents of the running configuration file.

Step 3	**`show call-manager-fallback all`**
	Example:
	`Router# 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.

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:
www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/index.htm

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:
  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
 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
 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/ATADefault.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 SEP003094C2772E.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP001201372DD1.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000001.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000002.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000003.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000004.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000005.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000006.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000007.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000008.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000009.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000A.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000B.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000C.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000D.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000E.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000F.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000010.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000011.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000012.cnf.xml
```

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**
4. **video**
5. **maximum bit-rate** *value*

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`call-manager-fallback`
	Example:
	`Router(config)# call-manager-fallback`
		Enters call-manager-fallback configuration mode.

Step 4	`video`
	Example:
	`Router(config-call-manager-fallback)# video`
		Enters call-manager-fallback video configuration mode.

Step 5	`maximum bit-rate` *value* **Example:** `Router(conf-cm-fallback-video)# maximum bit-rate 256`	Sets the maximum IP phone video bandwidth, in kbps. The range is 0 to 10000000. The default is 10000000.

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 cch323 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 (CCAPI).
- 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 ephone registered**: Displays the status of registered ephones.
  - **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

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

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Monitoring and Maintaining Cisco Unified SRST

Revised: July 11, 2008

To monitor and maintain Cisco Unified Survivable Remote Site Telephony (SRST), use the following commands in the privileged EXEC and mode.

Command	Purpose
`Router# show running-config`	Displays the configuration.
`Router# show call-manager-fallback all`	Displays the detailed configuration of all the Cisco Unified IP phones, voice ports, and dial peers of the Cisco Unified SRST Router.
`Router# show call-manager-fallback dial-peer`	Displays the output of the dial peers of the Cisco Unified SRST Router.
`Router# show call-manager-fallback ephone-dn`	Displays Cisco Unified IP Phone destination numbers when in call manager fallback mode.
`Router# show call-manager-fallback voice-port`	Displays output for the voice ports.
`Router# show ephone phone`	Displays Cisco Unified IP Phone status.
`Router# show ephone offhook`	Displays Cisco Unified IP Phone status for all phones that are off hook.
`Router# show ephone registered`	Displays Cisco Unified IP Phone status for all phones that are currently registered.
`Router# show ephone remote`	Displays Cisco Unified IP Phone status for all nonlocal phones (phones that have no Address Resolution Protocol [ARP] entry).
`Router# show ephone ringing`	Displays Cisco Unified IP Phone status for all phones that are ringing.
`Router# show ephone summary`	Displays a summary of all Cisco Unified IP Phones.
`Router# show ephone telephone-number phone-number`	Displays Unified IP Phone status for a specific phone number.
`Router# show ephone unregistered`	Displays Unified IP Phone status for all unregistered phones.
`Router# show ephone-dn tag`	Displays Unified IP Phone destination numbers.
`Router# show ephone-dn summary`	Displays a summary of all Cisco Unified IP Phone destination numbers.
`Router# show ephone-dn loopback`	Displays Cisco Unified IP Phone destination numbers in loopback mode.

Command	Purpose
`Router# show voice port summary`	Displays a summary of all voice ports.
`Router# show dial-peer voice summary`	Displays a summary of all voice dial peers.

Where to Go Next

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

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Enhanced 911 Services

Revised: July 11, 2008

This chapter describes the Enhanced 911 Services feature.

Finding Feature Information in This Module

Your Cisco Unified SRST 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 Enhanced 911 Services" section on page 263.

Contents

Prerequisites

- Cisco Unified SRST 4.1 or later versions
- SCCP or SIP phones must be registered to the Cisco Unified SRST server.
- At least one CAMA or ISDN trunk must be configured from Cisco Unified SRST to each of the 911 service provider's public safety answering point (PSAP).
- An Enhanced 911 network must be designed for each customer's voice network
- Cisco Unified SRST can use FXS, FXO, SIP, or H.323 trunk interfaces.

Restrictions

- 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.
- 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 the "Precautions for Mobile Phones" section on page 233.
- The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL). For more information, see the "Overview" section on page 228.
- 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" section on page 236.
- 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 SRST Features" section on page 236.

Information About Enhanced 911 Services

This section contains the following information about Enhanced 911 Services:

- Overview, page 228
- Call Processing, page 231
- New Features for Version 4.2(1), page 233
- Precautions for Mobile Phones, page 233
- Planning Your Implementation of Enhanced 911 Services, page 234
- Interactions with Existing Cisco Unified SRST Features, page 236

Overview

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.

To use Enhanced 911 Services, you must define an emergency response location (ERL) for each of the geographic areas needed to cover all of the phones supported by Cisco Unified SRST. The geographic specifications for ERLs are determined by local law. For example, you might have to define an ERL for each floor of a building because an ERL must be less than 7000 square feet in area. Because the ERL defines a known, specific location, this information is uploaded to the PSAP's database and is used by the 911 dispatcher to help the emergency response team to quickly locate a caller.

To determine which ERL is assigned to a 911 caller, the PSAP uses the caller's unique phone number, which is also known as the emergency location identification number (ELIN). Before you can use Enhanced 911 Services you must supply the PSAP with a list of your ELINs and street addresses for each ERL. This information is saved in the PSAP's automatic location identification (ALI) database. Typically, you give this information to the PSAP when your phone system is installed.

With the address information in the ALI database, the PSAP can find the caller's location and can also use the ELIN to callback the 911 caller within a specified time limit. This limit applies to the Last Caller table, which provides the PSAP with the 911 caller's ELIN. If no time limit is specified for the Last Caller table, the default expiry time is three hours.

In addition to saving call formation in the temporary Last Caller table, you can configure permanent call detail records. You can view the attributes in these records from RADIUS accounting, the syslog service, or CLI show commands.

You have the option of configuring zero, one, or two ELINs for each ERL. If you configure two ELINs, the system uses a round-robin algorithm to select which ELIN is sent to the PSAP. If you do not define an ELIN for an ERL, the PSAP sees the original calling number. You may not want to define an ELIN if Cisco Unified SRST is using direct-inward-dial numbers or the call is from another Cisco voice gateway that has already translated the extension to an ELIN.

Optionally define a default ELIN that the PSAP can use if a 911 caller's IP phone's address does not match the IP subnet of any location in any zone. This default ELIN can be an existing ELIN that is already defined for one of the ERLs or it can be a unique ELIN. If no default ELIN is defined and the 911 caller's IP Address does not match any of the ERLs' IP subnets, a syslog message is issued stating that no default ELIN is defined, and the original ANI remains intact.

You can also define a designated callback number that is used when the callback information is lost in the Last Caller table because of an expiry timeout or system restart or when the PSAP cannot reach the 911 caller at the caller's ELIN or the default ELIN for any other reason.

You can further customize your system by specifying the expiry time for data in the Last Caller table and by enabling syslog messages that announce all emergency calls

For large installations, you can optionally specify that calls from specific ERLs are routed to specific PSAPs. This is done by configuring emergency response zones, which lists the ERLs within each zone. This list of ERLs also includes a ranking of the locations which controls the order of ERL searches when there are multiple PSAPs. You do not need to configure emergency response zones if all 911 calls on your system are routed to a single PSAP.

One or more ERLs can be grouped into a zone which could be equivalent to the area serviced by a PSAP. When an outbound emergency call is placed, configured emergency response zones allow the searching of a subset of the ERLs in any order. The ERLs can be ranked in the order of required usage.

Zones are also used to selectively route 911 calls to different PSAPs.You can configure selective routing by creating a zone with a list of unique locations and assigning each zone to a different outbound dial peer. In this case, zones route the call based on the caller's ERL. When an emergency call is made, each dial peer matching the called number uses the zone's list of locations to find a matching IP subnet to the calling phone's IP address. If an ERL and ELIN are found, the dial peer's interface is used to route the call. If no ERL or ELIN is found, the next matched dial peer checks its zone.

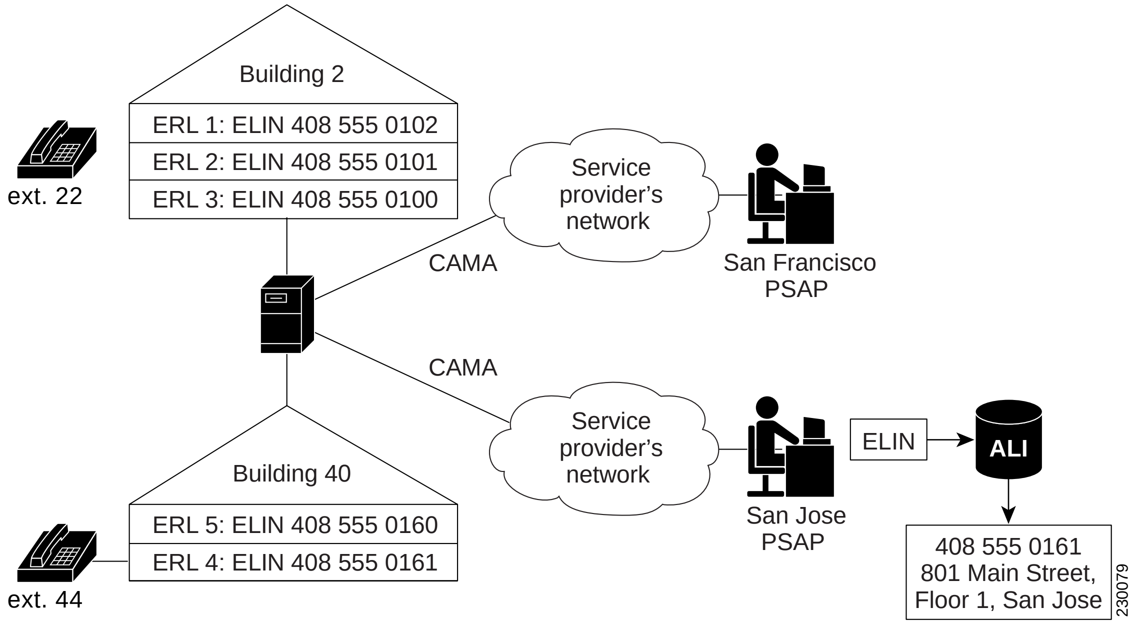
Note If a caller's IP address does not match any location in its dial peer's zone, the last dial peer that matched is used for routing and the default ELIN is used.

If you want 911 calls from any particular phone to always use the same dial peer when you have multiple dial peers going to the same destination-pattern (911) and the zones are different, you must configure the preferred dial peer to be the highest priority by setting the preference field.

Duplicate location tags are not allowed in the same zone. However, the same location tag can be defined in multiple zones. You are allowed to enter duplicate location priorities in the same zone, however, the existing location's priority is then increased to the next number. For example, if you configure "location 36 priority 5" followed by "location 19 priority 5," location 19 has priority 5 and location 36 becomes priority 6. Also, if two locations are assigned priority 100, rather than bump the first location to priority 101, the first location becomes the first nonprioritized location.

Figure 1 shows a an example configuration for 911 services. In this example, the phone system handles calls from multiple floors in multiple buildings. Five ERLs are defined, with one ELIN defined for each ERL. At the PSAP, the ELIN is used to find the caller's physical address from the ALI database. In this example, building 2 is closer to the PSAP in San Francisco and Building 40 is closer to the PSAP in San Jose. Therefore, in this case, we recommend that you configure two emergency response zones to ensure that 911 calls are routed to the PSAP closest to the caller. In this example, you can configure an emergency response zone that includes all of the ERLS in building 2 and another zone that includes the ERLs in building 40. If you choose to not configure emergency response zones, 911 calls will be routed based on matching with the destination number configured for the outgoing dial peers.

Figure 1 Implementation of Enhanced 911



Call Processing

When a 911 call is received by Cisco Unified SRST, the initial call processing is the same as for any other call. Cisco Unified SRST takes the called-number and searches for dial peers that can be used to route the call to that called-number.

The Enhanced 911 feature also analyzes the outgoing dial peer to see if it is going to a PSAP. If the outgoing dial peer is configured with the **emergency response zone** command, the system is notified that the call needs Enhanced 911 handling. If the outgoing dial peer is not configured with the **emergency response zone** command, the Enhanced 911 functionality is not activated and the caller's number is not translated to an ELIN.

When the Enhanced 911 functionality is activated, the first step in Enhanced 911 handling is to determine which ERL is assigned to the caller. There are two ways to determine the caller's ERL.

- Explicit Assignment — If a 911 call arrives on an inbound dial peer that has an ERL assignment, this ERL is automatically used as the caller's location.
- Implicit Assignment — If a 911 call arrives from an IP phone, its IP address is determined and Enhanced 911 searches for the IP address of the caller's phone in one of the IP subnets configured in the ERLs. The ERLs are stored as an ordered list according to their tag numbers, and each subnet is compared to the caller's IP address in the order listed.

After the caller's ERL is determined, the caller's number is translated to that ERL's ELIN. If no ERLs are implicitly or explicitly assigned to a particular call, you can define a default ERL for IP phones. This default ERL does not apply to nonIP-phone endpoints, such as phones on VoIP trunks or FXS/FXO trunks.

After an ELIN is determined for the call, the following information is saved to the Last Caller table:

- Caller's ELIN
- Caller's original extension
- Time the call originated

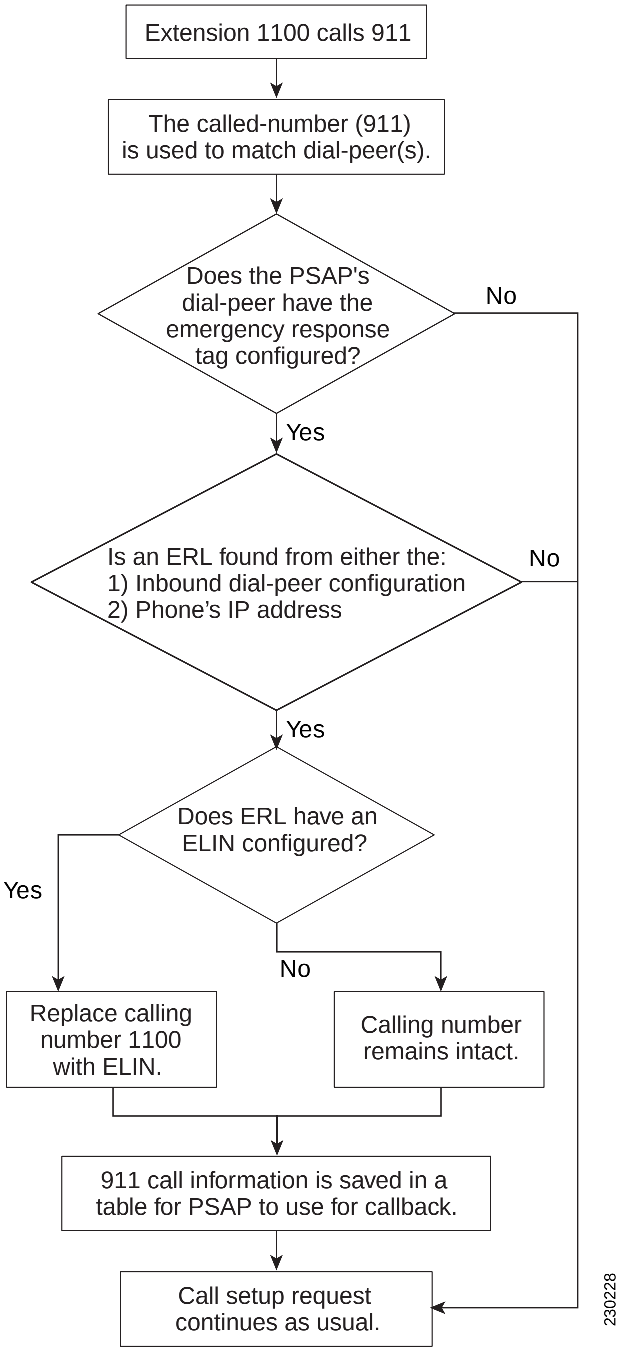
The Last Caller table contains this information for the most recent emergency callers from each ERL. A caller's information is purged from the table when the specified expiry time has passed after the call was originated. If no time limit is specified, the default expiry time is three hours.

After the 911 call information is saved to the Last Caller table, the system determines whether an emergency response zone is configured that contains the caller's ERL. If no emergency response zone is configured with the ERL, all ERLs are searched sequentially to match the caller's IP address and then route the 911 call to the appropriate PSAP. If an ERL is included in a zone, the 911 call is routed to the PSAP associated with that zone.

After the 911 call is routed to appropriate PSAP, Enhanced 911 processing is complete. Call processing then proceeds as it does for basic calls, except that the ELIN replaces the original calling number for the outbound setup request.

Figure 2 summarizes the procedure for processing a 911 call.

Figure 2 ***Processing a 911 Call***


Extension 1100 calls 911
The called-number (911) is used to match dial-peer(s).
Does the PSAP's dial-peer have the emergency response tag configured?
No
Yes
Is an ERL found from either the: 1) Inbound dial-peer configuration 2) Phone’s IP address
No
Yes
Does ERL have an ELIN configured?
Yes
No
Replace calling number 1100 with ELIN.
Calling number remains intact.
911 call information is saved in a table for PSAP to use for callback.
Call setup request continues as usual.
230228

The 911 operator is unable to find information about a call in the Last Caller table if the router was rebooted or specified expiry time (three hours by default) has passed after the call was originated. If this is the case, the 911 operator hears the reorder tone. To prevent the 911 operator from getting this tone, you can configure the default callback as described in the “Configuring Outgoing Dial Peers for Enhanced 911 Services” section on page 242. Alternately, you can configure a call forward number on the dial peer that goes to an operator or primary contact at the business.

Because the 911 callback feature tracks the last caller by its extension number, if you change the configuration of your ephone-dns in-between a 911 call and a 911 callback and within the expiry time, the PSAP might not be able to successfully contact the last 911 caller.

If two 911 calls are made from different phones in the same ERL within a short period of time, the first caller's information is overwritten in the Last Caller table with the information for the second caller. Because the table can contain information about only one caller from each ERL, the 911 operator does not have the information needed to contact the first caller.

In most cases, if Cisco Emergency Responder is configured, you should configure Enhanced 911 Services with the same data for the ELIN and ERL as used by Cisco Emergency Responder.

New Features for Version 4.2(1)

Version 4.2(1) of Enhanced 911 Services includes these new features:

- Assigning ERLs to zones to enable routing to the PSAP that is closest to the caller
- 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
- Expanding the E911 location information to include name and address
- Adding new permanent call detail records
- Adding new troubleshooting commands

Precautions for Mobile Phones

Emergency calls placed from phones that have been removed from their primary site might not be answered by local safety authorities. Do not use IP phones to place emergency calls if removed from the site where it was initially configured. Therefore, we recommend that you require your mobile phone users to agree to a policy similar to the one stated below.

Telecommuters, remote office, and traveling personnel must place emergency calls on a locally configured hotel, office, or home phone landline. If they must use a remote IP phone for emergency calls while away from their configured site, they must be prepared to provide specific information regarding their location (their country, city, state, street address, and so on) to the answering safety authority or security operations center personnel.

By accepting this policy your mobile phone users are confirming that they:

- Understand this advisory
- Agree to take reasonable precautions to prevent use of any remote IP phone device for emergency calls when it is removed from its configured site

By not responding to or declining to accept this policy, your mobile phone users are confirming that they understand that all remote IP phone devices associated with them will be disconnected, and no future requests for these services will be fulfilled.

Planning Your Implementation of Enhanced 911 Services

Before you configure Enhanced 911 Services for Cisco Unified SRST, plan your installation as described in the following procedure.

Note Some of the features described in this procedure are not available for all versions of Cisco Unified SRST. To determine whether a feature is available for your version, see the "New Features for Version 4.2(1)" section on page 233.

Step 1 Make a list of your sites that are serviced by Cisco Unified SRST, and the PSAPs serving each site.

Be aware that you must use a CAMA/PRI interface to connect to each PSAP. Table 1 shows an example of the information that you need to gather.

.

Table 1 Site and PSAP Information

Building Name and Address	Responsible PSAP	Interface to which Calls Are Routed
Building 2, 201 Maple Street, San Francisco	San Francisco, CA	Port 1/0:D
Building 40, 801 Main Street, San Jose	San Jose, CA	Port 1/1:D

Step 2 Use local laws to determine the number of ERLs you must configure.

According to the National Emergency Number Association (NENA) model legislation, make the location specific enough to provide a reasonable opportunity for the emergency response team to quickly locate a caller anywhere within it. Table 2 shows an example.

Table 2 ERL Calculation

Building	Size in Square Feet	Number of Floors	Number of ERLs Required
Building 2	200,000	3	3
Building 40	7000	2	1

Step 3 (Optional) Assign one or two ELINs to each ERL.

You must contact your phone service provider to request phone numbers that are designated as ELINs.

Step 4 (Optional) Assign each of your ERLs to an emergency response zone to enable 911 calls to be routed to the PSAP that is closest to the caller. Use the **voice emergency response zone** command.

Step 5 Configure one or more dial peers for your 911 callers with the **emergency response zone** command.

You might need to configure multiple dial peers for different destination-patterns.

Step 6 Configure one or more dial peers for the PSAP's 911 callbacks with the **emergency response callback** command.

Step 7 Decide what method to use to assign the phones to each ERL.

You have the following choices:

- For a group of phones that are on the same subnet, you can create an IP subnet in the ERL that includes each phone's IP address. Each ERL can have one or two unique IP subnets. This is the easiest option to configure. Table 3 shows an example.

Table 3 Example Settings for ERLs, Descriptions, IP Subnet Addresses, and ELINs

ERL Number	Description	IP Address Assignment	ELIN
1	Building 2, 1st floor	10.5.124.xxx	408 555-0142
2	Building 2, 2nd floor	10.7.xxx.xxx	408 555-0143
3 & 4	Building 2, 3rd floor	10.8.xxx.xxx and 10.9.xxx.xxx	408 555-0144 and 408 555-0145

- You can assign an ERL explicitly to a group of phones by using the ephone-template and voice register template configurations. Instead of assigning an ERL to phones individually, you can use these templates to save time if you want to apply the same set of features to several ephones or SIP phones.
- You can assign an ERL to a phone individually. Depending on which type of phone you have, you can use one of three methods. You can assign an ERL to a phone's:
  - Ephone configuration
  - Dial-peer configuration
  - Voice register pool configuration

  Table 4 shows examples of each of these options.

Table 4 Explicit ERL Assignment Per Phone

Phone Configuration	ERL
Ephone 100	3
Dial-peer voice 213 pots	3
Dial-peer voice 214 voip	4
Voice register pool 1	2

Step 8 (Optional) Define a default ELIN to be sent to the PSAP for use if a 911 caller's IP phone's address does not match the IP subnet of any location in any zone.

Step 9 (Optional) Define a designated callback number that is used if the callback information is removed from the Last Caller table because of an expiry timeout or system restart.

Step 10 (Optional) Change the expiry time for data in the Last Caller table from the default time of three hours.

Step 11 (Optional) Enable RADIUS accounting or the syslog service to permanently record call detail records.

Interactions with Existing Cisco Unified SRST Features

Enhanced 911 Services interacts with several existing Cisco Unified SRST features. The interactions with each of the following features are described in separate sections below:

Note Your version of Cisco Unified SRST might not support all of these features.

- Multiple Usages of an ELIN, page 236
- Number Translation, page 236
- Call Transfer, page 237
- Call Forward, page 237
- Call Blocking Features, page 237
- Call Waiting, page 237
- Three-Way Conference, page 238
- Dial-Peer Rotary, page 238
- Dial Plan Patterns, page 238
- Caller ID Blocking, page 238
- Shared Line, page 238

Multiple Usages of an ELIN

Caution We recommend that you do not use ELINs for any other purpose because of possible unexpected interactions with existing Cisco Unified SRST features.

Examples of using ELINs for other purposes include configuring an ELIN for use as an actual phone number (ephone-dn, voice register dn, FXS destination-pattern), a Call Pickup number, or an alias rerouting number.

Using ELINs as an actual phone number causes problems when calls are made to that number. If a 911 call occurs and the last caller information has not expired from the Last Caller table, any outside callers will reach the last 911 caller instead of the actual phone. We recommend that you do not share the phone numbers used for ELINs with real phones.

There is no impact on outbound 911 calls if you use the same number for an ELIN and a real phone number.

Number Translation

The Enhanced 911 feature translates the calling number to an ELIN during an outbound 911 call, and translates the called-number to the last caller's extension during a 911 callback (when the PSAP makes a callback to the 911 caller). Alternative methods of number translation can conflict with the translation done by the Enhanced 911 software, such as:

- Dialplan-pattern — Prefixes a pattern to an extension configured under telephony-service
- Num-exp — Expands extensions to full E.164 numbers

- Voice-port translation of called and calling numbers
- Outgoing number translation for dial peers
- Translate-profile for dial peers
- Voice translation profiles done for the dial peer, voice-port, POTS voice service, trunk group, trunk group member, voice source-group, call-manager-fallback, and ephone-dn
- Ephone-dn translation
- Voice register dn’s outgoing translation

Configuring these translation features impacts the Enhanced 911 feature if they translate patterns that are part of your ELINs’ patterns. For an outgoing 911 call, these features might translate an Enhanced 911 ELIN to a different number, giving the PSAP a number they cannot look-up in their ALI databases. If the 911 callback number (ELIN) is translated before Enhanced 911 callback processing, the Enhanced 911 feature is unable to find the last caller’s history.

Call Transfer

If a phone in a Cisco Unified SRST environment performs a semiattended or consultative transfer to the PSAP that involves another phone that is in a different ERL, the PSAP will use the wrong ELIN. The PSAP will see the ELIN of the transferor party, not the transferred party.

There is no impact on 911 callbacks (calls made by the PSAP back to a 911 caller) or transfers that are made by the PSAP.

A 911 caller can transfer the PSAP to another party if there is a valid reason to do so. Otherwise, we recommend that the 911 caller remain connected to the PSAP at all times.

Call Forward

There is no impact if an IP phone user calls another phone that is configured to forward calls to the PSAP.

If the PSAP makes a callback to a 911 caller that is using a phone that has Call Forward enabled, the PSAP is redirected to a party that is not the original 911 caller.

Call Blocking Features

Outbound 911 calls can be blocked by features such as After-Hours Call Blocking if the system administrator does not create an exception to 911 calls.

911 callbacks will not reach the 911 caller if the phone is configured with a blocking feature (for example, Do Not Disturb).

Call Waiting

After a 911 call is established with a PSAP, call waiting can interrupt the call. The 911 caller has the choice of putting the operator on hold. Although holding is not prohibited, we recommend that the 911 caller remain connected to the PSAP until the call is over.

Three-Way Conference

Although the 911 caller is allowed to activate three-way conferencing when talking to the PSAP, we recommend that the 911 caller remain connected privately to the PSAP until the call is over.

Dial-Peer Rotary

If a 911 caller uses a rotary phone, you must configure each dial peer with the **emergency response zone** command for the call to be processed as an Enhanced 911 call. Otherwise, calls received on dial peers that are not configured for Enhanced 911 functionality are treated as regular calls and there is no ELIN translation.

Do not configure two dial peers with the same destination-pattern to route to different PSAPs. The caller's number will not be translated to two different ELINs and the two dial peers will not route to different PSAPs. However, you can route calls to different PSAPs if you configure the dial peers with different destination-patterns (for example, 9911 and 95105558911). You might need to use the number translation feature or add prefix/forward-digits to change the 95105558911 to 9911 for the second dial peer if a specific called-number is required by the service provider.

Tip We recommend that you do not configure the same dial peer using both the **emergency response zone** and **emergency response callback** commands.

Dial Plan Patterns

Dial plan patterns expand the caller's original extension number into a fully qualified E.164 number. If an ERL is found for a 911 caller, the expanded number is translated to an ELIN.

For 911 callbacks, the called-number is translated to the 911 caller's expanded number.

Caller ID Blocking

When you set Caller ID Blocking for an ephone or voice-port configuration, the far-end gateway device blocks the display of the calling party information. This feature is overridden when an Enhanced 911 call is placed because the PSAP must receive the ELIN (the calling party information).

The Caller ID Blocking feature does not impact callbacks.

Shared Line

The Shared Line feature allows multiple phones to share a common directory number. When a shared line receives an incoming call, each phone rings. Only the first user that answers the call is connected to the caller.

The Shared Line feature does not affect outbound 911 calls.

For 911 callbacks, all phones sharing the directory number will ring. Therefore, someone who did not originate the 911 call might answer the phone and get connected to the PSAP. This could cause confusion if the PSAP needs to talk only with the 911 caller.

Configuring Enhanced 911 Services

This section contains the following:

- Configuring the Emergency Response Location, page 239 (required)
- Configuring Locations under Emergency Response Zones, page 241 (optional)
- Configuring Outgoing Dial Peers for Enhanced 911 Services, page 242 (required)
- Configuring a Dial Peer for Callbacks from the PSAP, page 246 (required)
- Assigning ERLs to Phones, page 247 (required)
- Configuring Customized Settings, page 251 (optional)
- Using the Address Command for Two ELINS, page 253 (optional)
- Enabling Call Detail Records, page 253 (optional)
- Verifying E911 Configuration, page 255 (optional)

Configuring the Emergency Response Location

The ERL can define zero, one, or two ELINs. If one ELIN is defined, this ELIN is always used for phones calling from this ERL. If you define two ELINs, the system alternates using each ELIN for phones calling from this ERL. If you define no ELINs and phones use this ERL, the outbound calls do not have their calling numbers translated. The PSAP sees the original calling numbers for these 911 calls.

If multiple ERLs are created, the Enhanced 911 software uses the ERL tag number to determine which ELIN to use. The Enhanced 911 software searches the ERLs sequentially from tag 1 to 2147483647. The first ERL that has a subnet mask encompassing the caller's IP address is used for ELIN translation.

Note The **voice emergency response location** command is expanded to include two new optional ERL fields, **name** and **address**. The **name** field provides a word or description of the ERL for administrative purposes. For example, **name** *Bldg 20 3rd floor* describes the purpose of an ERL configuration. The **address** field is a comma separated text entry of the ERL's civic address. The address is saved as part of the E911 ERL configuration. When used with the **show voice emergency addresses** command, the address information can be saved to a text file.

Prerequisites

- Plan your 911 configuration as described in "Planning Your Implementation of Enhanced 911 Services" section on page 234.
- Cisco Unified SRST Version 4.2(1) or Version 4.1 must be installed
- See the prerequisites described in the "Prerequisites" section on page 227

Restrictions

The **name** and **address** fields are not available for Cisco Unified SRST Version 4.1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice emergency response location** *tag*
4. **elin [1 | 2]** *E.164 number*
5. **address** *address*
6. **name** *name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice emergency response location** *tag* **Example:** `Router(config)# voice emergency response location 4`	Enters emergency response location configuration mode to define parameters for an ERL.
Step 4	**elin** *[1 | 2] E.164 number* **Example:** `Router(cfg-emrgncy-resp-location)# elin 1 4085550100`	(Optional) Specifies the ELIN, an E.164 PSTN number that replaces the caller's extension. This number is displayed on the PSAP's terminal and is used by the PSAP to query the ALI database to locate the caller. It is also used by the PSAP for callbacks. You can define a second ELIN using the optional **elin 2** command. If an ELIN is not defined for the ERL, the PSAP sees the original calling number.
Step 5	**address** *address* **Example:** `Router(cfg-emrgncy-resp-location)# address I,604,5550100, ,184 ,Main St,Kansas City,KS,1,`	(Optional) Defines a string used for the automatic location identification (ALI) database upload of the caller's address. The string must conform to the record format that is required by the service provider. The string maximum is 247 characters.

	Command or Action	Purpose
Step 6	**name** *name* **Example:** `Router(cfg-emrgncy-resp-location)# name Bldg C, Floor 2`	(Optional) Defines a 30-character string used internally to identify or describe the emergency response location.

Step 7	**end**
	Example:
	`Router(cfg-emrgncy-resp-location)# end`
		Returns to privileged EXEC mode.

Configuring Locations under Emergency Response Zones

In the configuration of emergency response zones, a list of locations within a zone is created using location tags. The zone configuration allows a ranking of the locations which controls the order of ERL searches when there are multiple PSAPs. The **zone** command is not used if all 911 calls on the system are routed to a single PSAP.

Prerequisites

- Define your ERLs as described in the "Configuring the Emergency Response Location" section on page 239.
- Cisco Unified SRST Version 4.2(1) must be installed

Restrictions

This feature is not available for Cisco Unified SRST Version 4.1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice emergency response zone** *tag*
4. **location** *location-tag* **[priority** *1-100***]**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice emergency response zone** *tag* **Example:** `Router(config)# voice emergency response zone 10`	Enters voice emergency response zone configuration mode to define parameters for an emergency response zone. The range is 1-100.
Step 4	**location** *location-tag* **[priority** *1-100***]** **Example:** `Router (cfg-emrgncy-resp-zone)# location 8 priority 2`	Each location tag must correspond to a location tag created using the **voice emergency response location** command. Repeat this command for each location included in the zone. Priority, which is optional, ranks the location in the zone list, 1 being the highest priority.

Step 5	**end**
	Example:
	`Router (config)# end`
		Returns to privileged EXEC mode.

Configuring Outgoing Dial Peers for Enhanced 911 Services

Depending on whether you decided to configure emergency response zones while you planned your 911 configuration as described in “Planning Your Implementation of Enhanced 911 Services” section on page 234, use one of the following procedures:

- If you decided to not use zones, see the “Configuring Outgoing Dial Peers for Enhanced 911 Services” section on page 242.
- If you decided to use zones, see the “Configuring Dial Peers for Emergency Response Zones” section on page 244.

Note The use of zones is not available for Cisco Unified SRST Version 4.1.

Configuring Dial Peers for Emergency Calls

Perform this procedure to create a dial peer for emergency calls to the PSAP. The destination-pattern of this dial peer is usually some variation of 911, such as 9911. This dial peer uses the port number of the CAMA or PRI network interface card. The new command **emergency response zone** specifies that this dial peer translates the calling number of any outgoing call's to an ELIN.

PREREQUISITES

Cisco Unified SRST Version 4.2(1) or Version 4.1 must be installed

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **pots**
4. **destination-pattern** *n***911**
5. **prefix** *number*
6. **emergency response zone**
7. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`dial-peer voice`** *`number`* **`pots`**
	Example:
	`Router(config)# dial-peer voice 911 pots`
		Enters dial-peer configuration mode to define parameters for an individual dial peer.

Step 4	**`destination-pattern_`***`n`***`911_`**
	Example:
	`Router(config-dial-peer)# destination-pattern 9911`
		Matches dialed digits to a telephony device. The digits included in this command specify the E.164 or private dialing plan telephone number. For Enhanced 911 Services, the digits are usually some variation of 911.

Step 5	**`prefix`** *`number`*
	Example:
	`Router(config-dial-peer)# prefix 911`
		(Optional) Includes a prefix that the system adds automatically to the front of the dial string before passing it to the telephony interface. For Enhanced 911 Services, the dial string is some variation of 911.

	Command or Action	Purpose
Step 6	**emergency response zone** **Example:** `Router(config-dial-peer)# emergency response zone`	Defines this dial peer as the one to use to route all ERLs defined in the system to the PSAP.

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

Configuring Dial Peers for Emergency Response Zones

In Cisco Unified SRST, you can selectively route a 911 call based on the ERL by assigning different zones to a dial peer. The **emergency response zone** command identifies the dial peer that routes the 911 call and the voice interface to use. The zone tag to this command allows only ERLs that are defined in that zone to be routed on the dial peer. Callers dialing the same emergency number are routed to different voice interfaces based on the zone that includes its ERL.

PREREQUISITES

- Define your ERLs and emergency response zones as described in:
  - Configuring the Emergency Response Location, page 239
  - Configuring Locations under Emergency Response Zones, page 241
- Cisco Unified SRST Version 4.2(1) must be installed

RESTRICTIONS

This feature is not available for Cisco Unified SRST Version 4.1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **pots**
4. **destination-pattern** *n***911**
5. **prefix** *number*
6. **emergency response zone** *tag*
7. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`dial-peer voice`** *`number`* **`pots`**
	Example:
	`Router(config)# dial-peer voice 911 pots`
		Enters dial-peer configuration mode to define parameters for an individual dial peer.

Step 4	**`destination-pattern`** *`n`***`911`**
	Example:
	`Router(config-dial-peer)# destination-pattern 9911`
		Matches dialed digits to a telephony device. The digits included in this command specify the E.164 or private dialing plan telephone number. For E911 services, the digits are usually some variation of 911.

Step 5	**`prefix number`**
	Example:
	`Router(config-dial-peer)# prefix 911`
		(Optional) Includes a prefix that the system adds automatically to the front of the dial string before passing it to the telephony interface. For E911 services, the dial string is some variation of 911.

Step 6	**`emergency response zone`** *`tag`*
	Example:
	`Router(config-dial-peer)# emergency response zone 10`
		Defines this dial peer as the one that is used to route ERLs defined for that zone.
		The tag points to an existing configured zone. The range is 1-100.

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

Configuring a Dial Peer for Callbacks from the PSAP

Perform this procedure to create a dial peer for 911 callbacks from the PSAP. This dial peer enables the PSAP to use the ELIN to make callbacks. When a call arrives that matches this dial peer, the **emergency response callback** command instructs the system to find the last caller that used the ELIN and translate the destination number of the incoming call to the extension of the last caller.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **pots**
4. **incoming called-number** *number*
5. **direct-inward-dial**
6. **emergency response callback**
7. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`dial-peer voice`** *number* **`pots`**
	Example:
	`Router(config)# dial-peer voice 100 pots`
		Enters dial-peer configuration mode to define parameters for an individual dial peer.

Step 4	**`incoming called-number`** *number* **Example:** `Router(config-dial-peer)# incoming called-number 4085550100`	(Optional) Selects the inbound dial peer based on the called number to identify the last caller. This number is the ELIN.

Step 5	**`direct-inward-dial`**
	Example:
	`Router(config-dial-peer)# direct-inward-dial`
		(Optional) Enables the Direct Inward Dialing (DID) call treatment for the incoming called number. For more information, see the *Cisco Voice, Video, and Fax Configuration Guide*.

	Command or Action	Purpose

Step 6	`emergency response callback`
	Example:
	`Router(config-dial-peer)# emergency response callback`
		Identifies a dial peer as an ELIN dial peer.

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

Assigning ERLs to Phones

Both versions of Cisco Unified SRST can use the same procedures to assign ERLs a phones. The type of phones that you have determines which of the following methods you will use, as explained in Step 7 in the "Planning Your Implementation of Enhanced 911 Services" section on page 234. Use one of the following procedures:

- To assign en ERLS to an IP subnet, see the "Assigning an ERL to a Phone's IP Subnet" section on page 248.
- To assign an ERL to a phone's ephone, see the "Assigning an ERL to a Phone's Ephone" section on page 249.
- To assign an ERL to a phone's dial peer, see the "Assigning an ERL to a Dial Peer" section on page 250.

Prerequisites

- Define your ERLs and emergency response zones as described in the "Configuring the Emergency Response Location" section on page 239.
- Cisco Unified SRST Version 4.2(1) or Version 4.1 must be installed

Assigning an ERL to a Phone's IP Subnet

Use this procedure typically when you have a group of phones that are on the same subnet. You can configure an ERL to be associated with one or two unique IP subnets. This indicates to the Enhanced 911 software that all IP phones that fall into a specific subnet will use the ELIN defined in this ERL.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice emergency response location** *tag*
4. **subnet [1 | 2]** *IPaddress mask*
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`voice emergency response location` *tag* **Example:** `Router(config)# voice emergency response location 4`	Enters emergency response location configuration mode to define parameters for an ERL.
Step 4	`subnet [1 | 2]` *IPaddress mask* **Example:** `Router(cfg-emrgncy-resp-location)# subnet 1 192.168.0.0 255.255.0.0`	Defines the groups of IP phones that are part of this location. You can create up to 2 different subnets. To include all IP phones on a single ERL, use the command **subnet 1 0.0.0.0 0.0.0.0** to configure a default subnet. This subnet does not apply to nonIP-phone endpoints, such as phones on VoIP trunks or FXS/FXO trunks.

Step 5	`end`
	Example:
	`Router(cfg-emrgncy-resp-location)# end`
		Returns to privileged EXEC mode.

Assigning an ERL to a Phone's Ephone

Perform this procedure if you chose to assign an ERL to a phone's ephone instead of configuring an ERL to be associated with IP subnets. For more information about this decision, see Step 7 in the "Planning Your Implementation of Enhanced 911 Services" section on page 234.

Note This method of assigning an ERL is available only for Cisco Unified SRST, not for Cisco Unified SIP SRST.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *tag*
4. **emergency response location** *tag*
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`ephone`** *tag* **Example:** `Router(config)# ephone 224`	Enters ephone configuration mode to define parameters for an individual ephone.
Step 4	**`emergency response location`** *tag* **Example:** `Router(config-ephone)# emergency response location 12`	Assigns an ERL to a phone's ephone configuration using an ERL's tag. The tag is an integer from 1 to 2147483647. If the ERL's tag is not a configured tag, the phone is not associated to an ERL and the phone defaults to its IP address to find the inclusive ERL subnet.

Step 5	**`end`**
	Example:
	`Router(config-ephone)# end`
		Returns to privileged EXEC mode.

Assigning an ERL to a Dial Peer

Perform this procedure to assign an ERL to a FXS/FXO or VoIP dial peer. Because these interfaces do not have IP addresses associated with them, you must use this procedure instead of configuring an ERL to be associated with IP subnets. For more information about this decision, see Step 7 in the "Planning Your Implementation of Enhanced 911 Services" section on page 234.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag type*
4. **emergency response location** *tag*
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`dial-peer voice`** *tag type* **Example:** `Router(config)# dial-peer voice 100 pots`	Enters dial peer configuration mode to define parameters for an individual dial peer.
Step 4	**`emergency response location`** *tag* **Example:** `Router(config-dial-peer)# emergency response location 12`	Assigns an ERL to a phone's dial peer configuration using an ERL's tag. The tag is an integer from 1 to 2147483647. If the ERL's tag is not a configured tag, no translation occurs and no Enhanced 911 information is saved to the last emergency caller table.

Step 5	**`end`**
	Example:
	`Router(config-dial-peer)# end`
		Returns to privileged EXEC mode.

Configuring Customized Settings

The E911 settings you can customize are:

- **Elin**: The default ELIN. If a 911 caller's IP phone address does not match the subnet of any location in any zone, the default ELIN is used to replace the original automatic number identification (ANI). The default ELIN can be already defined in one of the ERLs or can be unique. If a default ELIN is not defined and there is no match for the 911 caller's IP address, the PSAP sees the ANI for callback purposes. A syslog message is sent requesting the default ELIN, and no caller location information is available to the PSAP.
- **Expiry**: The number of minutes a 911 call is associated to an ELIN in case of a callback from the 911 operator. The callback expiry can be changed from a default of 3 hours to any time between 2 minutes and 48 hours. The timer is started the moment the 911 call goes to the PSAP. The PSAP can call back the ELIN and reach the last caller within this expiry time.
- **Callback:** The default phone number to contact if a 911 callback cannot find the last 911 caller from the Last Caller table. This can happen if the callback occurs after a router has rebooted or if the expiration has elapsed.
- **Logging**: A syslog informational message is printed to the console every time an emergency call is made. Such a message is required for third party applications to send an e-mail or page to an in-house emergency administrator. This is a default feature that can be disabled using the **no logging** command. The following is an example of a syslog notification message:

```
%E911-5-EMERGENCY_CALL_PLACED: calling #[4085550100] called
#[911] ELIN [4085550199]
```

Prerequisites

Cisco Unified SRST Version 4.2(1) must be installed

Restrictions

This feature is not available for Cisco Unified SRST Version 4.1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice emergency response settings**
4. **expiry** *time*
5. **callback** *number*
6. **logging**
7. **elin** *number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`voice emergency response settings`**
	Example:
	`Router(config)# voice emergency response settings`
		Enters voice emergency response settings mode to define settings you can customize for E911 calls.

Step 4	**`expiry`** *`time`*
	Example:
	`Router(cfg-emrgncy-resp-settings)# expiry 300`
		(Optional) Defines the time period (in minutes) that the emergency caller history information for each ELIN is stored in the Last Caller table. The time can be an integer in the range of 2 minutes to 2880 minutes. The default value is 180 minutes.

Step 5	**`callback`** *`number`*
	Example:
	`Router(cfg-emrgncy-resp-settings)# callback 7500`
		(Optional) Defines the E.164 callback number (for example, a company operator or main help desk) if a 911 callback cannot find the last caller associated to the ELIN.

Step 6	**`logging`**
	Example:
	`Router(cfg-emrgncy-resp-settings)# no logging`
		(Optional) Enables syslog messages that announce every emergency call. The syslog messages can be tracked to send pager or e-mail notifications to an in-house support number. By default, logging is enabled. Use the **no** form of this command to disable logging.

Step 7	**`elin`** *`number`*
	Example:
	`Router(cfg-emrgncy-resp-settings)# elin 4085550100`
		Specifies the E.164 number to be used as the default ELIN if no ERL has a subnet mask that matches the current 911 caller's IP phone address.

Step 8	**`end`**
	Example:
	`Router (cfg-emrgncy-resp-settings)# end`
		Returns to privileged EXEC mode.

Using the Address Command for Two ELINS

Note This feature is not available for Cisco Unified SRST Version 4.1.

For ERLs that have two ELINs defined, you cannot use just one **address** field to have two address entries for each ELIN in the ALI database. Instead of entering the specific phone number, a key phrase is entered to represent each ELIN. The **show voice emergency address** command produces output that replaces the key phrase with the ELIN information and generates two lines of addresses.

To define the expression, use the keyword *elin* (context-insensitive), followed by a period, the starting position of the ELIN to use, followed by another period, and finally the ending position of the ELIN. For example:

```
address I,ELIN.1.3,ELIN.4.7,678 ,Alder Drive ,Milpitas ,CA,95035
```

In the example, the second parameter of **address** following I are digits 1-3 of each ELIN. The third parameter are digits 4-7 of each ELIN. When you enter the **show voice emergency address** command, the output will replace the key phrase as seen in the following:

```
I,408,5550101,678,Alder Drive ,Milpitas ,CA,95035
I,408,5550190,678,Alder Drive ,Milpitas ,CA,95035
```

Enabling Call Detail Records

Note This feature is not available for Cisco Unified SRST Version 4.1.

To conform to internal policy or external regulations, you may be required to save 911 call history data including the following information:

- Original caller’s extension
- ELIN information
- ERL information (the integer tag and the text name)
- Original caller’s phone IP address

These attributes are visible from the RADIUS accounting server and syslog server output, or by using the **show call history voice** command.

Note You must enable the RADIUS server or the syslog server to display these details. See your RADIUS or syslog server documentation.

Output from a RADIUS Accounting Server

For RADIUS accounting, the emergency call information is under a feature-vsa record. The fields are:

- EMR: Emergency call
- CGN: Original calling number
- ELIN: Emergency line identification number; the translated number
- CDN: Called number
- ERL: Emergency response location tag number
- ERLN: Emergency response location name; the name entered for the ERL, if one exists
- CIP: Caller’s IP address; nonzero for implicit ERL assignments
- ETAG: ERL tag; nonzero for explicit ERL assignments

The following shows an output example from a RADIUS server:

```
*Jul 18 15:37:43.691: RADIUS: Cisco AVpair [1] 202 "feature-vsa=fn:EMR
,ft:07/18/2007 15:37:32.227,frs:0,fid:6,fcid:A2444CAF347B11DC8822F63A1B4078DE,
legID:57EC,cgn:6045550101,elin:6045550199,cdn:911,erl:2,erln:Fisco,cip:1.5.6.200,etag:0"
```

Output from a Syslog Server

If gateway accounting is directed to the syslog server, a VOIP_FEAT_HISTORY system message appears. The feature-vsa parameters are the same ones described for RADIUS accounting.

The following shows an output example from a syslog server:

```
*Jul 18 15:37:43.675: %VOIPAAA-5-VOIP_FEAT_HISTORY: FEAT_VSA=fn:EMR,ft:07/18/2007
15:37:32.227,frs:0,fid:6,fcid:A2444CAF347B11DC8822F63A1B4078DE,legID:57EC,cgn:6045550199,
elin:6045550100,cdn:911,erl:2,erln:ABCDEFGHIJKLMNOPQRSTUVWXYZ123,cip:1.5.6.200,etag:0,
bguid:A23F6AD7347B11DC881DF63A1B4078DE
```

Output from the show call history voice Command

View emergency call information on the gateway using **show call active voice** and **show call history voice**. Some emergency call information is already in existing fields. The original caller’s number is under *OriginalCallingNumber*. The ELIN is at *TranslatedCallingNumber*. The four new fields are the ERL, ERL name, the calling phone’s IP address, and any explicit ERL assignments. These fields only appear if an ELIN translation occurs. For example, any 911 calls from an ERL with no ELIN defined do not print the four emergency fields in the **show call** commands. If no ERLs match the calling phone and the default ELIN is used, the ERL field displays *No Match*.

The following shows an output example using the **show call history voice** command:

```
EmergencyResponseLocation=3 (Cisco Systems 3)
ERLAssignment=3
DeviceIPAddress=1.5.6.202
```

Verifying E911 Configuration

For Version 4.2(1) Only

New **show** commands are introduced to display E911 configuration or usage.

- Use the **show voice emergency** command to display IP addresses, subnet masks, and ELINs for each ERL.

```
Router# show voice emergency

EMERGENCY RESPONSE LOCATIONS
ERL               | ELIN 1     | ELIN2      | SUBNET 1        | SUBNET 2
1                 | 6045550101 |            | 10.0.0.0        | 255.0.0.0
2                 | 6045550102 | 6045550106 | 192.168.0.0     | 255.255.0.0
3                 |            | 6045550107 | 172.16.0.0      | 255.255.0.0
4                 | 6045550103 |            | 192.168.0.0     | 255.255.0.0
5                 | 6045550105 |            | 209.165.200.224 | 255.0.0.0
6 6045550198      |            | 6045550109 | 209.165.201.0   | 255.255.255.224
```

- Use the **show voice emergency addresses** command to display address information for each ERL.

```
Router# show voice emergency addresses

3850 Zanker Rd, San Jose,604,5550101
225 W Tasman Dr, San Jose,604,5550102
275 W Tasman Dr, San Jose,604,5550103
518 Bellew Dr,Milpitas,604,5550104
400 Tasman Dr,San Jose,604,5550105
3675 Cisco Way,San Jose,604,5550106
```

- Use the **show voice emergency all** command to display all ERL information.

```
Router# show voice emergency all

VOICE EMERGENCY RESPONSE SETTINGS
   Callback Number: 6045550103
   Emergency Line ID Number: 6045550155
   Expiry: 2 minutes
   Logging Enabled

EMERGENCY RESPONSE LOCATION 1
   Name: Cisco Systems 1
   Address: 3850 Zanker Rd, San Jose,elin.1.3,elin.4.10
   IP Address 1: 209.165.200.226 IP mask 1: 255.255.255.254
   IP Address 2: 209.165.202.129 IP mask 2: 255.255.0.0
   Emergency Line ID 1: 6045550180
   Emergency Line ID 2:
   Last Caller:  6045550188 [Jan 30 2007 16:05.52 PM]
   Next ELIN For Emergency Call: 6045550166

EMERGENCY RESPONSE LOCATION 3
   Name: Cisco Systems 3
   Address: 225 W Tasman Dr, San Jose,elin.1.3,elin.4.10
   IP Address 1: 209.165.202.133 IP mask 1: 255.255.0.0
   IP Address 2: 209.165.202.130 IP mask 2: 255.0.0.0
   Emergency Line ID 1:
   Emergency Line ID 2: 6045550150
   Last Caller:
   Next ELIN For Emergency Call: 6045550151
```

- Use the **show voice emergency zone** command to display each zone’s list of locations in order of priority.

```
Router# show voice emergency zone

EMERGENCY RESPONSE ZONES
 zone 90
    location 4
    location 5
    location 6
    location 7
    location 2147483647
 zone 100
    location 1 priority 1
    location 2 priority 2
    location 3 priority 3
```

For Version 4.1 and Version 4.2(1)

Use the **show voice emergency callers** command to see the translations made by outbound 911 calls. This command lists the originating number, the ELIN used, and the time for each 911 call. This history is active for only three hours after the call is placed. Expired calls are not shown in this output.

```
router# show voice emergency callers
EMERGENCY CALLS CALL BACK TABLE
ELIN                      | CALLER                     | TIME
6045550100                | 6045550150                 | Oct 12 2006 03:59:43
6045550110                | 8155550124                 | Oct 12 2006 04:05:21
```

Troubleshooting Enhanced 911 Services

Step 1 Use the **debug voice application error** and the **debug voice application callsetup** command. These are existing commands for calls made using the default session or TCL applications.

This example shows the debug output when a call to 911 is made:

```
router# debug voice application error
router# debug voice application callsetup

Nov 10 23:49:05.855: //emrgncy_resp_xlate_callingNum: InDialPeer[20001], OutDialPeer[911]
callingNum[6046692003]
Nov 10 23:49:05.855: //ER_HistTbl_Find_CallHistory: 6046699100
Nov 10 23:49:05.855: //59//Dest:/DestProcessEmergencyCall: Emergency Call detected: Using
ELIN 6046699100
```

This example shows the debug output when a PSAP calls back an emergency caller:

```
router# debug voice application error
router# debug voice application callsetup

Nov 10 23:49:37.279: //emrgncy_resp_xlate_calledNum: calledNum[6046699100],
dpeerTag[6046699]
Nov 10 23:49:37.279: //ER_HistTbl_Find_CallHistory: 6046699100
Nov 10 23:49:37.279: //HasERHistoryExpired: elapsedTime[10 minutes]
Nov 10 23:49:37.279: //67//Dest:/DestProcessEmergencyCallback: Emergency Response
Callback: Forward to 6046692003.
Nov 10 23:49:37.279: //67//Dest:/DestCaptureCallForward: forwarded to 6046692003 reason 1
```

Error Messages

The Enhanced 911 feature introduces a new system error message. The following error message displays if a 911 callback cannot route to the last 911 caller because the saved history was lost because of a reboot, an expiration of an entry, or a software error:

```
%E911_NO_CALLER:  Unable to contact last 911 caller.
```

Configuration Examples for Enhanced 911 Services

For Version 4.2(1) Only

Emergency response settings are:

- default elin if no elin match is found: 604 555-0120
- expiry time for information in the Last Caller table: 180 minutes
- callback number if the PSAP operator must call back the 911 caller and the call back history has expired: 604 555-0199

Zone 1 has four locations, 1, 2, 3, and 4, and a name, address, and elin are defined for each location. Each of the four locations is assigned a priority. In this example, because location 4 has been assigned the highest priority, it is the first that is searched for IP subnet matches to identify the ELIN assigned to the 911 caller’s phone. A dial peer is configured to route 911 calls to the PSAP (voice port 1/0/0). Callback dial peers are also configured.

```
voice emergency response settings
elin 6045550120
expiry 180
callback 6045550199

voice emergency response location 1
name Bldg C, Floor 1
address I,604,5550135, ,184 ,Main St,Kansas City,KS,1,
elin 1 6045550125
subnet 1 172.16.0.0 255.255.0.0
!
voice emergency response location 2
name Bldg C, Floor 2
address I,elin.1.3,elin.4.7, ,184 ,Main St,Kansas City,KS,2,
elin 1 6045550126
elin 2 6045550127
subnet 1 192.168.0.0 255.255.0.0
!
voice emergency response location 3
name Bldg C, Floor 3
address I,604,5550138, ,184 ,Main St,Kansas City,KS,3,
elin 2 6045550128
subnet 1 209.165.200.225 255.255.0.0
subnet 2 209.165.200.240 255.255.0.0
!
voice emergency response location 4
name Bldg D
address I,604,5550139, ,192 ,Main St,Kansas City,KS,
elin 1 6045550129
subnet 1 209.165.200.231 255.255.0.0
```

```
!
voice emergency response zone 1
location 4 priority 1
location 3 priority 2
location 2 priority 3
location 1 priority 4
!
dial-peer voice 911 pots
description Public Safety Answering Point
emergency response zone 1
destination-pattern 911
port 1/0/0
!
dial-peer voice 6045550 voip
emergency response callback
destination-pattern 6045550...
session target loopback:rtp
codec g711ulaw
!
dial-peer voice 1222 pots
emergency response location 4
destination-pattern 6045550130
port 1/0/1
!
dial-peer voice 5550144 voip
emergency response callback
session target ipv4:1.5.6.10
incoming called-number 604555....
codec g711ulaw
!
```

For Version 4.1 and Version 4.2(1)

In this example, Enhanced 911 Services is configured to assign an ERL to the following:

- The 10.20.20.0 IP subnet
- Two dial peers
- A SIP phone

```
Router#show running-config

Building configuration...

Current configuration : 6241 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
hostname rm-uut3-2821
!
boot-start-marker
boot-end-marker
!
no aaa new-model
network-clock-participate wic 1
network-clock-participate wic 2
no network-clock-participate wic 3
!
```

```
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool sccp-7912-phone1
    host 10.20.20.122 255.255.0.0
    client-identifier 0100.1200.3482.cd
    default-router 10.20.20.3
    option 150 ip 10.21.20.218
!
ip dhcp pool sccp-7960-phone2
    host 10.20.20.123 255.255.0.0
    client-identifier 0100.131a.a67d.cf
    default-router 10.20.20.3
    option 150 ip 10.21.20.218
    dns-server 10.20.20.3
!
ip dhcp pool sip-phone1
    host 10.20.20.121 255.255.0.0
    client-identifier 0100.15f9.b38b.a6
    default-router 10.20.20.3
    option 150 ip 10.21.20.218
!
ip dhcp pool sccp-7960-phone1
    host 10.20.20.124 255.255.0.0
    client-identifier 0100.14f2.37e0.00
    default-router 10.20.20.3
    option 150 ip 10.21.20.218
    dns-server 10.20.20.3
!
!
no ip domain lookup
ip host rm-uut3-c2821 10.20.20.3
ip host RescuMe01 10.21.20.218
multilink bundle-name authenticated
!
isdn switch-type basic-net3
!
!
voice service voip
  allow-connections h323 to h323
  allow-connections h323 to sip
  allow-connections sip to h323
  allow-connections sip to sip
  supplementary-service h450.12
  sip
   registrar server
!
!
voice register global
  system message RM-SIP-SRST
  max-dn 192
  max-pool 48
!
voice register dn  1
  number 32101
!
voice register dn  185
  number 38301
!
voice register dn  190
  number 38201
!
voice register dn  191
```

```
  number 38202
!
voice register dn  192
  number 38204
!
voice register pool  1
  id mac DCC0.2222.0001
  number 1 dn 1
  emergency response location 2100
!
voice register pool  45
  id mac 0015.F9B3.8BA6
  number 1 dn 185
!
voice emergency response location 1
  elin 1 22222
  subnet 1 10.20.20.0 255.255.255.0
!
voice emergency response location 2
  elin 1 21111
  elin 2 21112
!
!
voice-card 0
  no dspfarm
!
!
archive
  log config
  hidekeys
!
!
controller T1 0/1/0
  framing esf
  linecode b8zs
  pri-group timeslots 8,24
!
controller T1 0/1/1
  framing esf
  linecode b8zs
  pri-group timeslots 2,24
!
controller T1 0/2/0
  framing esf
  clock source internal
  linecode b8zs
  ds0-group 1 timeslots 2 type e&m-immediate-start !
controller T1 0/2/1
  framing esf
  linecode b8zs
  pri-group timeslots 2,24
!
!
translation-rule 5
  Rule 0 ^37103 1
!
!
translation-rule 6
  Rule 6 ^2 911
!
!
interface GigabitEthernet0/0
  ip address 31.20.0.3 255.255.0.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 10.20.20.3 255.255.0.0
  duplex auto
  speed auto
!
interface Serial0/1/0:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-5ess
  isdn incoming-voice voice
  no cdp enable
!
interface Serial0/1/1:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-net5
  isdn incoming-voice voice
  no cdp enable
!
interface Serial0/2/1:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-net5
  isdn incoming-voice voice
  no cdp enable
!
interface BRI0/3/0
  no ip address
  isdn switch-type basic-5ess
  isdn twait-disable
  isdn point-to-point-setup
  isdn autodetect
  isdn incoming-voice voice
  no keepalive
!
interface BRI0/3/1
  no ip address
  isdn switch-type basic-5ess
  isdn point-to-point-setup
!
!
ip http server
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/1/0:23
!
voice-port 0/2/0:1
!
voice-port 0/1/1:23
!
voice-port 0/2/1:23
!
voice-port 0/3/0
!
voice-port 0/3/1
!
!
dial-peer voice 2002 pots
```

```
  shutdown
  destination-pattern 2....
  port 0/2/0:1
  forward-digits all
!
dial-peer voice 2005 pots
  description for-cme2-408-pri
  emergency response location 2000
  shutdown
  incoming called-number 911
  direct-inward-dial
  port 0/2/1:23
  forward-digits all
!
dial-peer voice 2004 voip
  description for-cme2-408-thru-ip
  emergency response location 2000
  shutdown
  session target loopback:rtp
  incoming called-number 911
!
dial-peer voice 1052 pots
  description 911callbackto-cme2-3
  shutdown
  incoming called-number .....
  direct-inward-dial
  port 0/1/1:23
  forward-digits all
!
dial-peer voice 1013 pots
  description for-analog
  destination-pattern 39101
  port 0/0/0
  forward-digits all
!
dial-peer voice 1014 pots
  description for-analog-2
  destination-pattern 39201
  port 0/0/1
  forward-digits all
!
dial-peer voice 3111 pots
  emergency response Zone
  destination-pattern 9....
  port 0/1/0:23
  forward-digits all
!
dial-peer voice 3121 pots
  emergency response callback
  incoming called-number 2....
  direct-inward-dial
  port 0/1/0:23
  forward-digits all
!
!
call-manager-fallback
  max-conferences 8 gain -6
  transfer-system full-consult
  ip source-address 10.20.20.3 port 2000
  max-ephones 3
  max-dn 3 dual-line preference 1
  system message primary SRST-UUT3-2851
  keepalive 45
!
```

```
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
!
end

rm-uut3-2821#$
```

Feature Information for Enhanced 911 Services

Table 5 lists the enhancements to the Enhanced 911 Services feature by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified SRST version, see the *Cisco Unified Communications Manager Compatibility Matrix* at the following URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/docguide/6_1_2/dg612.html#wp1028473.

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.

Note Table 5 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 5 Feature Information for Enhanced 911 Services

Feature Name	Releases	Feature Information
Updates for Enhanced 911 Services	4.2(1)	• Assign ERLs to zones • Define a default ELIN, add a designated callback number, change the expiry time for data in the Last Caller table, enable syslog messages that announce emergency calls • Add name and address information to 911 caller data • Add new call detail records • Add new troubleshooting commands
Enhanced 911 Services	4.1	Enhanced 911 Services was introduced.

Where to Go Next

For information about monitoring and maintaining Cisco Unified SRST, go to the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

Appendix A: Preparing Cisco Unified SRST Support for SIP

Revised: July 11, 2008

Cisco Unified Survivable Remote Site Telephony (SRST) supports incoming and outgoing Session Initiation Protocol (SIP) calls to and from Cisco Unified IP phones and router voice gateway voice ports, but does not support direct attachment of SIP phones to Cisco Unified SRST. 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).

Special configurations to support SIP calls are described in this appendix. For more information about SIP, see the *Cisco IOS SIP Configuration Guide*.

Contents

DTMF Relay for SIP Applications and Voice Mail

DTMF relay for SIP applications can be used in two voice-mail situations:

- DTMF Relay Using SIP RFC 2833, page 265
- DTMF Relay Using SIP Notify (Nonstandard), page 267

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 voice-mail 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 voice-mail 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 voice-mail 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

	Command or Action	Purpose
Step 1	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode.
Step 2	**dtmf-relay rtp-nte** **Example:** `Router(config-dial-peer)# dtmf-relay rtp-nte`	Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.
Step 3	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.
Step 4	**sip-ua** **Example:** `Router(config)# sip-ua`	Enables SIP user-agent configuration mode.

	Command or Action	Purpose
Step 5	`notify telephone-event max-duration` *time* **Example:** `Router(config-sip-ua)# notify telephone-event max-duration 2000`	Configures the maximum time interval allowed between two consecutive NOTIFY messages for a single DTMF event. • **max-duration** *time*: Time interval between consecutive NOTIFY messages for a single DTMF event, in milliseconds. Range is from 500 to 3000. Default is 2000.

Step 6	`exit`
	Example:
	`Router(config-sip-ua)# exit`
		Exits SIP user-agent configuration mode.

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:

```
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 voice mail 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.

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

	Command or Action	Purpose
Step 1	**dial-peer voice** *tag* **voip** **Example:** Router(config)# dial-peer voice 2 voip	Enters dial-peer configuration mode.
Step 2	**dtmf-relay sip-notify** **Example:** Router(config-dial-peer)# dtmf-relay sip-notify	Forwards DTMF tones using SIP NOTIFY messages.
Step 3	**exit** **Example:** Router(config-dial-peer)# exit	Exits dial-peer configuration mode.
Step 4	**sip-ua** **Example:** Router(config)# sip-ua	Enables SIP user-agent configuration mode.
Step 5	**notify telephone-event max-duration** *time* **Example:** Router(config-sip-ua)# notify telephone-event max-duration 2000	Configures the maximum time interval allowed between two consecutive NOTIFY messages for a single DTMF event. • **max-duration** *time*: Time interval between consecutive NOTIFY messages for a single DTMF event, in milliseconds. Range is from 500 to 3000. Default is 2000.
Step 6	**exit** **Example:** Router(config-sip-ua)# exit	Exits SIP user-agent configuration mode.

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
Redirection (3xx) message handling:ENABLED

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

Where to Go Next

For information about monitoring and maintaining Cisco Unified SRST, go to the “Monitoring and Maintaining Cisco Unified SRST” section on page 225.

For additional information, see the “Additional References” section on page 46 in the “Overview of Cisco Unified SRST” section on page 33.

INDEX