Cisco Unified Communications Manager Express System Administrator Guide

Last Modified: 2017-11-30

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

CONTENTS

CHAPTER 1

Cisco Unified CME Features Roadmap

This roadmap lists the features documented in the *Cisco Unified Communications Manager Express System Administrator Guide* and maps them to the modules in which they appear.

Feature and Release Support

Table 1: Supported Cisco Unified CME Features, on page 1 lists the Cisco Unified Communications Manager Express (Cisco Unified CME) version that introduced support for a given feature. Unless noted otherwise, subsequent versions of Cisco Unified CME software also support that feature. Only features that were introduced or modified in Cisco Unified CME 4.0 or a later version appear in the table. *Not all features may be supported in your Cisco Unified CME software version*.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. An account on Cisco.com is not required.

Table 1: Supported Cisco Unified CME Features

Version	Feature Name	Feature Description	Where Documented
Unified CME 12.1			
	No New features added in the Unified CME 12.1 Release.		
Unified CME 12.0			
	New Phone Support	As part of Unified CME Release 12.0, new phone support for Cisco IP Phones 8821, 8845, 8865 was introduced for Cisco Integrated Services Router Generation 2. The support is introduced for T-Train Release Version, 15.7(3)M and later.	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST

Version	Feature Name	Feature Description	Where Documented
	Idle URL for SIP Phones	Support for Idle URL feature was introduced for SIP Phones, as part of Unified CME Release 12.0	Information About Cisco Unified IP Phone Options, on page 1437
	Calling Number Local	Support to configure Calling Number Local under voice register global configuration mode was introduced as part of Unified CME Release 12.0.	Calling Number Local, on page 1170
	Called-Name Display (Dialed Number Identification Service)	Support to configure Dialed Number Identification Service for phones configured under voice hunt group was introduced as part of Unified CME Release 12.0.	Called-Name Display, on page 660
	cBarge on Mixed Shared Lines	Support for cBarge functionality in a mixed deployment scenario was introduced as part of Unified CME Release 12.0.	Barge and Privacy, on page 1047
Unified CME 11.7			
11.7	New Phone Support	As part of Unified CME Release 11.7, new phone support for Cisco IP Phones 8821, 8845, 8865 was introduced. With this addition, Unified CME supports all phone models in Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series.	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST
	Transcoding support for Music on Hold	Transcoding for MOH is supported on Cisco 4000 Series Integrated Services Router from Cisco Unified CME Release 11.7 onwards.	Music on Hold, on page 829

Version	Feature Name	Feature Description	Where Documented
	Support for Conferencing on Unified CME	Provides support for conferencing on Cisco 4000 Series Integrated Services Router from Cisco Unified CME Release 11.7 onwards.	Conferencing, on page 1369
	Support for Cisco Smart License	Provides support for Smart Licensing apart from the existing CSL licensing model from Cisco Unified CME Release 11.7 onwards.	Cisco Unified CME Overview, on page 67
Unified CME 11.6			
11.6	Extension Assigner for SIP Phones	Provides support for automatically synchronizing configuration changes to backup systems for SIP Phones.	Create Phone Configurations Using Extension Assigner, on page 347
	Call Transfer Recall for SIP Phones	Support for call transfer recall functionality on SIP phones.	Call Transfer Recall on SIP Phones, on page 1159
	Secondary Unified CME for SIP Phones	**Failover to Redundant Router**—Sites can be set up with a primary and secondary Cisco Unified CME router to provide redundant Cisco Unified CME capability. SIP Phones automatically register at the secondary router if the primary router fails and later rehome to the primary router when it is operational again.	Redundant Cisco Unified CME Router for SIP Phones, on page 161

Version	Feature Name	Feature Description	Where Documented
	VHG Enhancements	Support for voice hunt group features such as Hlog support on SIP phone, DND Softkey as Hlog, Members Logout, Auto Logout, Presentation of calls, and Dynamic Agent Join or Unjoin Status message display on SIP phones.	Call Coverage Features, on page 1239 Customize Softkeys, on page 925
	Night Service (Mixed Mode)	Support for night service functionality in a mixed deployment scenario.	Call Coverage Features, on page 1239
	Secondary Dial Tone for SIP Phones	Support for Secondary Dial Tone on SIP Phones.	Configure Dial Plans, on page 451
	BACD with Loopback call flows	Support to invoke B-ACD services when calling from a local SIP, SCCP or FXS phone.	http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/bacd/configuration/guide/cme40tcl/40bacd.html
	Transcoding Support on Unified CME	Support for LTI-based Transcoding on Cisco 4000 Series Integrated Services Router.	Transcoding Support, on page 474
Cisco Unified CME 11.5			
11.5	Auto Registration	Support for auto registration of SIP phones on Unified CME. Introduced the CLI command auto-register in voice register global mode to enable automatic registration of SIP phones on Unified CME.	Auto Registration of SIP Phones on Cisco Unified CME, on page 235
	Night Service	Support for night service functionality on SIP phones.	Night Service, on page 1271
	B-ACD	Support for B-ACD functionality on SIP phones.	Cisco Unified CME B-ACD and Tcl Call-Handling Applications

Version	Feature Name	Feature Description	Where Documented
Cisco Unified CME 11.0			
11.0	New Phone Support	Lists the new phones that have been provided with support on Unified CME: • Support for Cisco IP Phone 7811 • Support for Cisco IP Phones 8811, 8831, 8841, 8851, 8851NR, 8861 • Support for Cisco ATA-190 Phones	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST
Cisco Unified CME 10.5			
10.5	New Phone Support	Lists the new phones that have been provided with support on Unified CME: • Support for Cisco Unified 78xx Series SIP IP Phones • Support for Cisco DX650	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST
	Example for Monitoring the Status of Key Expansion Modules	Monitoring the Status of Key Expansion Modules: Example section has been updated to include support the show summary commands.	Example for Monitoring the Status of Key Expansion Modules, on page 337
	Monitoring and Maintaining Cisco Unified CME	Monitoring and Maintaining Cisco Unified CME table has been updated to include the new show commands introduced in this release.	Cisco IOS Commands for Monitoring and Maintaining Cisco Unified CME, on page 339
	Localization Enhancements in Cisco Unified CME	Localization Enhancement feature recommends User-Defines locales.	Localization Enhancements in Cisco Unified CME, on page 407

Version	Feature Name	Feature Description	Where Documented
	Fast Dial	Fast Dial range has been increased to 100.	Enable a Personal Speed Dial Menu on SCCP Phones, on page 972
	Viewing Active Parked Calls	Viewing Active Parked Calls feature enables the user to view the list of active parked calls on SIP and SCCP phones.	View Active Parked Calls, on page 1083
	Distinctive Ring	Distinctive Ring feature enables the user to distinctly identify the type of call.	Call Park Recall Enhancement, on page 1088
	Viewing and Joining Voice Hunt Groups	Viewing and Joining Voice Hunt Groups feature enables the user to view voice hunt group related information on SIP and SCCP phones.	View and Join for Voice Hunt Groups, on page 1253
	Dynamically Joining or Unjoining Multiple Voice Hunt Groups	Dynamically Joining or Unjoining Multiple Voice Hunt Groups feature provides support for phones to dynamically join the voice hunt groups is added.	Dynamically Join or Unjoin Multiple Voice Hunt Groups, on page 1265
	Audible Tone	The Audible Tone feature has been introduced on SCCP phones to enable the user to receive a confirmation on successful log in or log out from an ephone hunt group and voice hunt group.	Enable Audible Tone for Successful Login and Logout of a Hunt Group on SCCP Phone, on page 1309
	Cisco Jabber Client Support on CME	A new phone type, 'Jabber-CSF-Client' has been added to configure the Cisco Jabber client under voice register pool.	Cisco Jabber Client Support on CME, on page 1443

Version	Feature Name	Feature Description	Where Documented
	Multi VRF Support	Multi VRF Support feature has been enhanced to provide support for SIP phones.	Example for Configuring Multi- VRF Support for Cisco Unified CME SIP Phones, on page 1568
Cisco Unified CME 10.0			
10.0	Fast-Track Configuration Approach for Cisco Unified SIP IP Phones	Fast-Track Configuration feature provides a new configuration utility using which you can input the phone characteristics of a new SIP phone model.	Fast-Track Configuration Approach for Cisco Unified SIP IP Phones, on page 251
	Cisco Jabber for Microsoft Windows	Cisco Jabber for Windows client is supported from Cisco Unified CME Release 10 onwards.	Cisco Jabber Client Support on CME, on page 1443
	Cisco Unified CME-SRST License	Cisco Unified CME-SRST permanent license has been introduced along with new license package called Collaboration Professional Suite.	Licenses, on page 69
	Secure SIP Trunk Support on Cisco Unified CME	Supports supplementary services in secure SRTP and SRTP fallback modes on SIP trunk of the SCCP Cisco Unified CME.	Secure SIP Trunk Support on Cisco Unified CME, on page 593
Cisco Unified CME 9.5			
9.5	Afterhours Pattern Blocking Support for Regular Expressions	Support for afterhours pattern blocking is extended to regular expression patterns for dial plans on Cisco Unified SIP and Cisco Unified SCCP IP phones.	After-Hours Pattern-Blocking Support for Regular Expressions, on page 1062

Version	Feature Name	Feature Description	Where Documented
	Call Park Recall Enhancement	The recall force keyword is added to the **call-park system** command in telephony-service configuration mode to allow a user to force the recall or transfer of a parked call to the phone that put the call in park.	Call Park Recall Enhancement, on page 1088
	Display Support for Name of Called Voice Hunt Groups	The display of the name of the called voice-hunt-group pilot is supported by configuring the following command in voice hunt-group or ephone-hunt configuration mode: [**no**] **name** *primary pilot name* [**secondary** *secondary pilot name*]	Display Support for the Name of a Called Voice Hunt-Group, on page 1259
	Enhancement of Support for Hunt Group Agent Statistics	Support for hunt group agent statistics of Cisco Unified SCCP IP phones is enhanced to include the following information: • Total logged in time—On an hourly basis, displays the duration (in sec) since a specific agent logged into a hunt group. • Total logged out time—On an hourly basis, displays the duration (in sec) since a specific agent logged out of a hunt group.	Enhancement of Support for Ephone-Hunt Group Agent Statistics, on page 1261

Version	Feature Name	Feature Description	Where Documented
	HTTPS Support in Cisco Unified CME	With Hypertext Transfer Protocol Secure (HTTPS) support in Cisco Unified CME 9.5 and later versions, these services can be invoked using an HTTPS connection from the phones to Cisco Unified CME.	HTTPS Provisioning For Cisco Unified IP Phones, on page 596
	Localization Enhancements in Cisco Unified CME	Canadian French is supported as a user-defined locale on Cisco Unified SIP IP phones and Cisco Unified SCCP IP phones when the correct locale package is installed.	Localization Enhancements in Cisco Unified CME, on page 407
	Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups	Local calls are prevented from being forwarded to the final destination using the **no forward local-calls to-final** command in parallel or sequential voice hunt-group configuration mode.	Prevent Local Call Forwarding to the Final Agent in a Voice Hunt-Groups, on page 1260
	Support for Voice Hunt Group Descriptions	A description can be specified for a voice hunt group using the **description** command in voice hunt-group configuration mode.	Support for Voice Hunt Group Descriptions, on page 1260
	Trunk to Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones Cisco Unified CME 9.0	Trunk to trunk transfer blocking for toll bypass fraud prevention is supported on Cisco Unified Session Initiation Protocol (SIP) IP phones also.	Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones, on page 1151
Cisco Unified CME 9.0			

Version	Feature Name	Feature Description	Where Documented
9.1	KEM Support for Cisco Unified 8961, 9951, and 9971 SIP IP Phones	Increases line key and feature key appearances, speed dials, or programmable buttons on Cisco Unified SIP IP phones.	
9.0	Cisco ATA-187	Supports T.38 fax relay and fax pass-through on Cisco ATA-187.	Configure Cisco ATA Support, on page 295
	Cisco Unified SIP IP Phones	Adds SIP support for the following phone types: • Cisco Unified 6901 and 6911 IP Phones • Cisco Unified 6921, 6941, 6945, and 6961 IP Phones • Cisco Unified 8941 and 8945 IP Phones	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST

Version	Feature Name	Feature Description	Where Documented
	Localization Enhancements for Cisco Unified SIP IP Phones	Provides the following enhanced localization support for Cisco Unified SIP IP phones: • Localization support for Cisco Unified 6941 and 6945 SIP IP Phones. • Locale installer that supports a single procedure for all Cisco Unified SIP IP phones.	Localization Support for Cisco Unified SIP IP Phones, on page 409
	MIB Support for Extension Mobility in Cisco Unified SCCP IP Phones	Adds new MIB objects to monitor Cisco Unified SCCP IP Extension Mobility (EM) phones.	MIB Support for Extension Mobility in Cisco Unified SCCP IP Phones, on page 729
	Mixed Shared Lines	Allows Cisco Unified SIP and SCCP IP phones to share a common directory number.	Mixed Shared Lines, on page 231
	Multiple Calls Per Line	Overcomes the limitation on the maximum number of calls per line.	Multiple Calls Per Line, on page 246
	My Phone Apps for Cisco Unified SIP IP Phones	Adds support for My Phone Apps feature on Cisco Unified SIP IP phones.	My Phone Apps for Cisco Unified SIP IP Phones, on page 1445
	Olson Timezone		Olson Timezones, on page 122

Version	Feature Name	Feature Description	Where Documented
		Eliminates the need to update time zone commands or phone loads to accommodate a new country with a new time zone or an existing country whose city or state wants to change their time zone, using the **olsontimezone** command in either telephony-service or voice register global configuration mode.	
	Paging Group Support for Cisco Unified SIP IP Phones	Allows you to specify a paging-dn tag and dial the paging extension number to page the Cisco Unified SIP IP phone associated with the paging-dn tag or paging group using the **paging-dn** command in voice register pool or voice register template configuration mode.	Paging Group Support for Cisco Unified SIP IP Phones, on page 859
	Programmable Line Keys for Cisco Unified SIP IP Phones	Adds support for softkeys as programmable line keys on Cisco Unified 6911, 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones.	Programmable Line Keys (PLK), on page 929
	Single Number Reach for Cisco Unified SIP IP Phones		Single Number Reach for Cisco Unified SIP IP Phones, on page 909

Version	Feature Name	Feature Description	Where Documented
		Supports the following SNR features for Cisco Unified SIP IP phones: • Enable and disable the EM feature. • Manual pull back of a call on a mobile phone. • Send a call to a mobile PSTN phone. • Send a call to a mobile phone regardless of whether the SNR phone is the originating or the terminating side.	
	Unsolicited Notify for Shared Line and Presence Events for Cisco Unified SIP IP Phones	Allows the Unsolicited Notify mechanism to reduce network traffic during Cisco Unified SIP IP phone registration using the bulk registration method.	Unsolicited Notify for Shared Line and Presence Events for Cisco Unified SIP IP Phones, on page 165
	Virtual SNR DN for Cisco Unified SCCP IP Phones	Allows a call to be made to a virtual SNR DN and allows the SNR feature to be launched even when the SNR DN is not associated with any phone.	Virtual SNR DN for Cisco Unified SCCP IP Phones, on page 910
	Voice Hunt Group Enhancements	Allows all ephone and voice hunt group call statistics to be written to a file using the **hunt-group statistics write-all** command.	Hunt Groups, on page 1248
Cisco Unified CME 8.8			

Version	Feature Name	Feature Description	Where Documented
	CTI CSTA Protocol Suite Enhancement	Enables the dial-via-office functionality from computer-based CSTA client applications and adds support to CSTA services and events.	CTI CSTA in Cisco Unified CME, on page 1519
	HFS Download Support for IP Phone Firmware and Configuration Files	Provides download support for SIP and SCCP IP phone firmware, scripts, midlets, and configuration files using the HTTP File-Fetch Server (HFS) infrastructure.	HFS Download Support for IP Phone Firmware and Configuration Files, on page 157
	HTTPS Provisioning for Cisco Unified IP Phones	Allows you to import an IP phone's trusted certificate to an IP phone's CTL file using the **import certificate** command.	HTTPS support for an External Server, on page 597
	Localization Enhancement	Adds localization support for Cisco Unified 3905 SIP and Cisco Unified 6945, 8941, and 8945 SCCP IP Phones.	System-Defined Locales, on page 408
	Programmable Line Keys Enhancement	Adds support for softkeys as programmable line keys on Cisco Unified 6945, 8941, and 8945 SCCP IP Phones.	Programmable Line Keys (PLK), on page 929
	Real-Time Transport Protocol Call Information Display Enhancement	Allows you to display information on active RTP calls using the **show ephone rtp connections** command. The output from this command provides an overview of all the connections in the system, narrowing the criteria for debugging pulse code modulation and Cisco Unified CME packets without a sniffer.	Real-Time Transport Protocol Call Information Display Enhancement, on page 248

Version	Feature Name	Feature Description	Where Documented
	SIP Intercom	Adds intercom support to Cisco Unified SIP phones connected to a Cisco Unified CME system.	SIP Intercom, on page 785
	Support for Cisco Unified 3905 SIP IP Phones	Adds support for SIP phones connected to a Cisco Unified CME system.	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST
	Support for Cisco Unified 6945, 8941, and 8945 SCCP IP Phones	Adds support for SCCP phones connected to a Cisco Unified CME system.	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST
Cisco Unified CME 8.6			
8.6	Bulk Registration Support for SIP Phones	Adds support for SIP phone bulk registration.	Bulk Registration Support for SIP Phones, on page 149

Version	Feature Name	Feature Description	Where Documented
	Clear Directory Entries in Missed/Placed/Received Calls List Support for iPhone and iPod Touch Softphone Client	Adds ability to clear phone call logs. Adds support for SIP client software for iPhone and iPod Touch.	Clear Directory Entries, on page 1437 Support for Cisco Jabber, on page 1442
	Enhancement for Call-Forward Unregistered	Adds support for the CFU feature on SIP IP phones using the **call-forward b2bua unregistered** command under voice register dn tag.	Call Forward Unregistered, on page 1148
	Extension Mobility Support for SIP phone	Adds SIP phone support to extension mobility.	Extension Mobility for SIP Phones Enhancement, on page 728
	Increase in the Number of Translation Rules	Increases the number of translation rules from 15 to 100 rules per translation rule table.	Define Translation Rules for Callback-Number on SIP Phones, on page 466
	Localization Support for SIP IP Phones	Adds localization support for SIP IP phones.	Localization Support for Cisco Unified SIP IP Phones, on page 409 Multiple Locales, on page 410 Configure Localization Support on SCCP Phones, on page 411 Configure Multiple Locales on SIP Phones, on page 434
	SSL VPN SUPPORT on CUCME with DTLS	Adds enhanced SSL VPN support. Cisco Unified SCCP IP phones such as 7945, 7965, and 7975 located outside of the corporate network are able to register to Cisco Unified CME through an SSL VPN connection.	SSL VPN Support on Cisco Unified CME with DTLS, on page 1009 Configure SSL VPN Client with DTLS on Cisco Unified CME as VPN Headend, on page 1031

Version	Feature Name	Feature Description	Where Documented
	Support for 7926G Wireless SCCP IP Phone	Adds support for 7926G Wireless SCCP IP Phone.	Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST
	Video Conferencing and Transcoding	Allows you to use on-board Digital Signal Processor resources (PVDM3) to facilitate adhoc or meetme video conference calls.	Transcoding Resources, on page 473
	Video and Camera Support for Cisco Unified IP Phones 8961, 9951, and 9971	Adds video support for IP phones 8961, 9951, and 9971.	SIP Endpoint Video and Camera Support for Cisco Unified IP Phones 8961, 9951, and 9971, on page 992
Cisco Unified CME 8.5			

Version	Feature Name	Feature Description	Where Documented
8.5	Customized Button Layout	Allows you to customize the display order of various button types on a phone using the button layout feature. The button layout feature allows you to customize the display of the following button types: • Line buttons • Speed Dial buttons • BLF Speed Dial buttons • Feature Buttons • ServiceURL buttons	Configure Button Layout on SCCP Phones, on page 1454 Configure Button Layout on SIP Phones, on page 1456
	Customized Phone User Interface Services	Allows to customize the availability of individual service items such as Extension Mobility, My Phone Apps, and Single Number Reach (SNR) on a phone's user interface by assigning an individual service item to a button using the Programmable Line Key (PLK) **url-button** command.	Customized Phone User Interface Services, on page 1439
	E.164 Enhancements	Allows to present a phone number in + E.164 telephone numbering format. E.164 is an International Telecommunication Union (ITU-T) recommendation that defines the international public telecommunication numbering plan used in the PSTN and other data networks.	E .164 Enhancements, on page 448

Version	Feature Name	Feature Description	Where Documented
	Enhancement to Voice Hunt Group Restriction	Allows you to ignore the timeout value for voice hunt group member and the call forward no answer timer when **call forward noan** command is configured in a voice hunt group.	Configure Call Coverage Features, on page 1278
	Feature Policy Softkey Control	Allows you to control softkeys on the Cisco Unified SIP IP Phones 8961, 9951, and 9971 using the feature policy template. The feature policy template allows you to enable and disable a list of feature softkeys on Cisco Unified SIP IP Phones 8961, 9951, and 9971.	Feature Policy Softkey Control, on page 928
	Forced Authorization Code	Allows you to manage call access and call accounting through the Forced Authorization Code (FAC) feature. The FAC feature regulates the type of call a certain caller may place and forces the caller to enter a valid authorization code on the phone before the call is placed. FAC allows you to track callers dialing non-toll-free numbers, long distance numbers, and also for accounting and billing purposes.	Forced Authorization Code, on page 763
	Immediate Divert for SIP Phones		Configure Immediate Divert (iDivert) Softkey on SIP Phone, on page 949

Version	Feature Name	Feature Description	Where Documented
		Allows you to immediately divert a call to a voice messaging system. You can divert a call to a voice messaging system by pressing the iDivert softkey on Cisco Unified SIP IP phones, such as 7940, 7040G, 7960 G, 7945, 7965, 7975, 8961, 9951, and 9971, with voice messaging systems (Cisco Unity Express or Cisco Unity).	
	Media Flow Around Support for SIP-SIP Trunk Calls	Eliminates the need to terminate RTP and re-originate on Cisco Unified CME through the media flow around feature, reducing media switching latency and increasing the call handling capacity for Cisco Unified CME SIP trunks.	Enable Media Flow Mode on SIP Trunks, on page 205
	Overlap Dialing Support for SIP and SCCP IP Phones	Enables overlap dialing on SCCP and SIP IP phones such as, 7942, 7945, 7962, 7965, 7970, 7971, and 7975.	Example for Configuring Overlap Dialing for SCCP IP Phones, on page 217
	Park Monitor	Allows you to park a call and monitor the status of the parked call until the parked call is retrieved or abandoned. When a Cisco Unified SIP IP Phone 8961, 9951, or 9971 parks a call using the **park** softkey, the park monitoring feature monitors the status of the parked call.	Park Monitor, on page 1088
	Phone User Interface for BLF-Speed-Dial		Enable BLF-Speed-Dial Menu, on page 888

Version	Feature Name	Feature Description	Where Documented
		Allows extension mobility (EM) users to configure dn-based Busy Lamp Field (BLF)-speed-dial settings directly on the phone through the Services feature button. BLF-speed-dial settings are added or modified (changed or deleted) on the phone using a menu available with the Services button.	
	Programmable Line Keys (PLK)	Allows you to program feature buttons or URL services button on phone's line keys. You can configure line keys as line buttons, speed dials, BLF speed dials, feature buttons, and URL buttons.	Programmable Line Keys (PLK), on page 929
	SNR Enhancements	Adds enhanced Single Number Reach feature for Cisco Unified CME: • Hardware Conference • Call Park, Call Pickup, and Call Retrieval • Answer Too Soon Timer • SNR Phone Stops Ringing After Mobile Phone Answers	Configure Single Number Reach Enhancements on SCCP Phones, on page 915
	SSL VPN Client Support on SCCP IP Phones	Enables Secure Sockets Layer (SSL) Virtual Private Network (VPN) on SCCP IP phones such as 7945, 7965, and 7975.	SSL VPN Client for SCCP IP Phones, on page 1009

Version	Feature Name	Feature Description	Where Documented
	XML API for Cisco Unified CME	Adds support for eXtensible Markup Language (XML) Application Programming Interface (API).	XML API for Cisco Unified CME, on page 1574
Cisco Unified CME 8.1			
8.1	Toll Fraud Prevention	Enables Toll Fraud Prevention on Cisco Unified CME to secure the Cisco Unified CME system against potential toll fraud exploitation by unauthorized users.	Toll Fraud Prevention, on page 511
	Enhancements to SIP Phone Configuration	Allows you to verify SIP phone registration process, remove global registration parameters, and display details on phones that attempted to register with Cisco Unified CME and failed.	Cisco Unified CME Commands: show presence global through subnet.
	Support for Cisco Unified 6901 and 6911 SCCP IP Phones	Adds support for new SCCP IP phones 6901 and 6911.	Ephone-Type Parameters for Supported Phone Types, on page 258
Cisco Unified CME 8.0(1)			

Version	Feature Name	Feature Description	Where Documented
8.0	Cancel Call Waiting	Enables an SCCP phone user to disable Call Waiting for a call they originate.	Call Coverage Features, on page 1239
	CTI CSTA Protocol Suite	Allows computer-based CSTA client applications, such as a Microsoft Office Communicator (MOC) client, to monitor and control the Cisco Unified CME system to enable programmatic control of SCCP telephony devices registered in Cisco Unified CME.	CTI CSTA Protocol Suite, on page 1519
	IPv6 Support for SCCP Endpoints	Adds IPv6 support for SCCP phones. SCCP Phones can interact with and support any SCCP devices that support IPv4 only or both IPv4 and IPv6 (dual-stack).	Configure IP Phones in IPv4, IPv6, or Dual Stack Mode, on page 167
	Logical Partitioning Class of Restriction (LPCOR)	Enables a single directory number on an IP or analog phone that is registered to Cisco Unified CME to connect to both PSTN and VoIP calls according to restrictions specified by Telecom Regulatory Authority of India (TRAI) regulations.	Call Restriction Regulations, on page 1101
	MLPP enhancements		Configure MLPP, on page 813

Version	Feature Name	Feature Description	Where Documented
		Adds enhanced Multilevel Priority and Preemption (MLPP) features for Cisco Unified CME including: • Additional MLPP announcements for isolated code (ICA), unauthorized precedence level (UPA), loss of C2 features (LOC2), and vacant code (VCA) • Multiple service domains for the Defense Switched Network (DSN) and Defense Red Switched Network (DRSN) • Route codes and service digits in dialing formats • Support for supplementary services, such as Three-Way Conferencing, Call Pickup, and Cancel Call Waiting on Analog FXS ports	
	Music On Hold Enhancement	Adds support for Music on Hold from different media sources.	Configure Music on Hold Groups to Support Different Media Sources, on page 842
	Secure IP Phone (IP-STE) Support	Adds support for secure IP Phone, IP-STE.	Internet Protocol - Secure Telephone Equipment Support, on page 242
Cisco Unified CME 7.1			

Version	Feature Name	Feature Description	Where Documented
7.1	Autoconfiguration of Cisco VG202, VG204, and VG224	Allows you to automatically configure the Cisco VG202, VG204, and VG224 Analog Phone Gateway from Cisco Unified CME.	
	Barge and cBarge for SIP Phones	Enables phone users to join a call on a SIP shared-line directory number.	Barge and Privacy, on page 1047
	BLF Monitoring of Ephone-DNs with DND, Call Park, Paging, and Conferencing	Provides Busy Lamp Field (BLF) indicators for directory numbers that become DND-enabled or are configured as call-park slots, paging numbers, or conference numbers.	Presence Service, on page 875
	BLF Monitoring of Devices	Supports device-based BLF monitoring, allowing a watcher to monitor the status of a phone, not only a line on the phone.	Presence Service, on page 875
	Busy Trigger and Channel Huntstop for SIP Phones	Provides a busy trigger and channel huntstop for directory numbers on SIP phones to prevent incoming calls from overloading the phone.	
	Call Park Enhancements	Adds Call Park features for SIP phones and enhances the Directed Call Park feature.	
	Call Pickup Enhancements	Adds Call Pickup features for SIP phones and enables users to perform Directed Call Pickup using the GPickUp softkey.	Call Coverage Features, on page 1239

Version	Feature Name	Feature Description	Where Documented
	DND Enhancement for SIP phones	Modifies DND behavior so that the SIP phone flashes an alert to visually indicate an incoming call instead of ringing and the call can be answered if desired.	Do Not Disturb, on page 679
	DSCP	Supports Differentiated Services Code Point (DSCP) packet marking for Cisco Unified IP phones.	
	Privacy for SIP phones	Enables phone users to block other users from seeing call information or barging into a call on a SIP shared-line directory number.	Barge and Privacy, on page 1047
	Shared-Line Directory Numbers	Adds shared-line directory numbers for SIP phones.	
	Single Number Reach (SNR)	Enables users to answer incoming calls on their desktop IP phone or at a remote destination, such as a mobile phone.	Configure Single Number Reach, on page 911
	SIP Trunk Video Support for SCCP Endpoints	Supports video calls between SCCP endpoints across different Cisco Unified CME routers connected through a SIP trunk. Supports H.264 codec for video calls.	Video Support, on page 987
	Whisper Intercom	Provides a one-way voice path from the caller to the called party, regardless of whether the called party is busy or idle. The called phone automatically answers in speakerphone mode.	Intercom Lines, on page 783

Version	Feature Name	Feature Description	Where Documented
Cisco Unified CME 7.0(1)			

Version	Feature Name	Feature Description	Where Documented
7.0(1)	**Note** Cisco Unified CME 7.0 includes the same features as Cisco Unified CME 4.3, which is renumbered to align with Cisco Unified Communications versions.		Configure System-Level Parameters, on page 167 Upgrade or Downgrade SCCP Phone Firmware, on page 107
	Cisco Unified CME Usability Enhancement	Automatically creates TFTP bindings using the enhanced **load** command if cnf location is router flash memory or router slot 0 memory.	
		• Introduces locale installer that supports a single procedure for all SCCP IP phones. • Automatically creates the required TFTP aliases for localization. • Provides backward compatibility with the configuration method in Cisco Unified CME 7.0 and earlier versions.	
	Cisco Unified CME TAPI Enhancement	Introduces a Cisco IOS command that disassociates and reestablishes a TAPI session that is in frozen state or out of synchronization.	Reset and Restart Cisco Unified IP Phones, on page 397
	Cisco Unity Express AXL Enhancement	Automatically synchronizes Cisco Unified CME and Cisco Unity Express passwords.	Voice Mail Integration, on page 539
	Cisco Unified IP Phones		

Version	Feature Name	Feature Description	Where Documented
		Adds SCCP support for the following phone type: Cisco Unified Communications Manager Express 7.0/4.3 Supported Firmware, Platforms, Memory, and Voice Products • Cisco Unified Wireless IP Phone 7925	Cisco Unified Communications Manager Express 7.0/4.3 Supported Firmware, Platforms, Memory, and Voice Products
	VRF Support on Cisco Unified CME	Adds support for conferencing, transcoding, a RSVP components in Cisco Unified CME through a VRF; also allows soft phones and TAPI clients in data VRF resources to communicate with phones in a VRF voice gateway.	Configure VRF Support, on page 1556
Cisco Unified CME 7.0/4.3			

Version	Feature Name	Feature Description	Where Documented
7.0/4.3	Autoprovisioning Directory Numbers in SRST Fallback Mode	Allows you to specify whether Cisco Unified CME in SRST Fallback mode creates octo-line or dual-line directory numbers for ephone-dns that are "learned" automatically from the ephone configuration.	SRST Fallback Mode, on page 1539
	Barge	Enables phone users to join a call on a shared octo-line directory number by pressing the Cbarge softkey and converting the call to an ad hoc conference.	Configure Barge and Privacy, on page 1050
	Call Transfer Recall	Enables a transferred call to return to the phone that initiated the transfer if the destination does not answer.	

Version	Feature Name	Feature Description	Where Documented
	Cisco 3200 Series Mobile Access Router	Support for Cisco Unified CME on the Cisco 3200 Series Mobile Access Router was added.	
	Cisco Unified IP Phones	Adds SCCP support for the following phone types: • Cisco Unified IP Phone 7915 Expansion Module • Cisco Unified IP Phone 7916 Expansion Module • Cisco Unified IP Conference Station 7937 • Nokia E61 Adds SIP support for the following phone types: • Cisco Unified IP Phone 7942G and 7945G • Cisco Unified IP Phone 7962G and 7965G • Cisco Unified IP Phone 7975G	Cisco Unified Communications Manager Express 7.0/4.3 Supported Firmware, Platforms, Memory, and Voice Products
	Consultative Transfer Enhancements		

Version	Feature Name	Feature Description	Where Documented
		Modifies the digit-collection process for consultative call transfers. After a phone user presses the Transfer softkey for a consultative transfer, a new consultative call leg is created and the Transfer softkey is not displayed again until the dialed digits of the transfer-to number are matched to a transfer pattern and consultative call leg is in alerting state.	
	Directory Search Enhancement	Increases the number of entries supported in a search results list from 32 to 240 when using the directory search feature.	Directory Services, on page 659
	Extension Mobility Enhancement	Adds support for the following: • Automatic Logout, including: ◦ Configurable time-of-day timers for automatically logging out all EM users. ◦ Configurable idle-duration timer for logging out a single user from an idle EM phone. ◦ Automatic Clear Call History when a user logs out from EM.	Extension Mobility, on page 725

Version	Feature Name	Feature Description	Where Documented
	Phone-Type Configuration	Allows you to dynamically add a new phone type to your configuration without upgrading your Cisco IOS software.	
	Live Record	Enables IP phone users to record a phone conversation when Cisco Unity Express is the voice mail system.	Voice Mail Integration, on page 539
	Maximum Ephones	Sets the maximum number of SCCP phones that can register to Cisco Unified CME using the **max-ephones** command, without limiting the number that can be configured. This enhancement also expands the maximum number of phones that can be configured to 1000.	
	Octo-Line Directory Numbers	Adds octo-line directory numbers that support up to eight active calls, both incoming and outgoing, on a single phone button. Unlike a dual-line directory number, an octo-line directory number can split its channels among other phones that share the directory number.	

Version	Feature Name	Feature Description	Where Documented
	Privacy	Enables phone users to block other users from seeing call information or barging into a call on a shared octo-line directory number.	Configure Barge and Privacy, on page 1050
	Push-to-Talk	Adds support for one-way Push-to-Talk (PTT) in Cisco Unified CME without requiring an external server to support the functionality. PTT is supported in firmware version 1.0.4 and later versions on Cisco Unified wireless IP phones with a thumb button.	Configure One-Way Push-to-Talk on Cisco Unified SCCP Wireless IP Phones, on page 1483
	Speed Dial/Fast Dial Phone User Interface	Allows IP phone users to configure their own speed-dial and fast-dial settings directly from the phone. Extension Mobility users can add or modify speed-dial settings in their user profile after logging in.	Speed Dial, on page 965
	Transfer to Voice Mail	Allows a phone user to transfer a call directly to a voice-mail extension by pressing the TrnsfVM softkey.	Voice Mail Integration, on page 539
	Voice Hunt-Group Enhancements		Call Coverage Features, on page 1239

Version	Feature Name	Feature Description	Where Documented
		Supports the following Voice Hunt Group features: • Call Forwarding to a Parallel Voice Hunt-Group (Blast Hunt Group). • Call Transfer to a Voice Hunt-Group. • Member of Voice Hunt-Group can be a SCCP phone, FXS analog phone, DS0-group, PRI-group, SIP phone, or SIP trunk.	
Cisco Unified CME 4.2(1)			
4.2(1)	Call Blocking Enhancements	Adds support for selective call blocking on IP phones and PSTN trunk lines.	Call Blocking, on page 1061
	Extension Assigner Synchronization	Provides support for automatically synchronizing configuration changes to backup systems.	Create Phone Configurations Using Extension Assigner, on page 347
	Extension Mobility Phone User support in Cisco Unified CME GUI	Allows a phone user to use a name and password from an EM profile to log into the Cisco Unified CME GUI for configuring personal speed dials on an EM phone. EM options in the GUI cannot be accessed from the System Administrator or Customer Administrator login screens.	Access the Cisco Unified CME GUI, on page 528
Cisco Unified CME 4.2			

Version	Feature Name	Feature Description	Where Documented
4.2	Enhanced 911 Services	• Enables routing to the PSAP closest to the caller by assigning ERLs to zones. • Allows you to customize E911 services by defining a default ELIN, designated number for callback, expiry time for Last Caller table, and syslog messages for emergency calls. • Expands the E911 location information to include name and address. • Uses templates to assign ERLs to a group of phones. • Adds permanent call detail records.	Enhanced 911 Services, on page 687
	Extension Mobility	Provides the benefit of phone mobility for end users by enabling the user to log into any local Cisco Unified IP phone that is enabled for extension mobility.	Extension Mobility, on page 725

Version	Feature Name	Feature Description	Where Documented
	Interoperability with Cisco Unified Contact Center Express (Cisco UCCX)	Enables interoperability between Cisco Unified CME and Cisco Customer Response Solutions (CRS) 5.0 and later versions with Cisco Unified Contact Center Express (Unified CCX), including Cisco Unified IP IVR, enhanced call processing, device and call monitoring, and unattended call transfers to multiple call center agents and basic extension mobility.	Interoperability with Cisco Unified CCX, on page 1495
	Media Encryption (SRTP) on Cisco Unified Communications Manager Express	Provides the following secure voice call capabilities: • Secure call control signaling and media streams in Cisco Unified CME networks using Secure Real-Time Transport Protocol (SRTP) and H.323 protocols. • Secure supplementary services for Cisco Unified CME networks using H.323 trunks. • Secure Cisco VG224 Analog Phone Gateway endpoints.	Security, on page 581
Cisco Unified CME 4.1			

Version	Feature Name	Feature Description	Where Documented
4.1	Call Forward All Synchronization	When a user enables Call Forward All on a SIP phone using the CfwdAll softkey, the uniform resource identifier (URI) for the service is sent to Cisco Unified CME. When Call Forward All is configured in Cisco Unified CME, the configuration is sent to the SIP phone which updates the CfwdAll softkey to indicate that Call forward All is enabled.	

Version	Feature Name	Feature Description	Where Documented
	Cisco Unified IP Phones	Adds SCCP support for the following phones: • Cisco Unified IP Phone 7921G • Cisco Unified IP Phone 7942G and 7945G • Cisco Unified IP Phone 7962G and 7965G • Cisco Unified IP Phone 7975G Adds SIP support for the following phones: • Cisco Unified IP Phone 3911 • Cisco Unified IP Phone 3951 • 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 7971G-GE No additional configuration is required for these phones. They are supported in the appropriate Cisco IOS commands.	Cisco Unified CME 4.1 Supported Firmware, Platforms, Memory, and Voice Products
	Directory Services	Supports local directory and local speed dial features for SIP phones.	Directory Services, on page 659

Version	Feature Name	Feature Description	Where Documented
	Disabling SIP Supplementary Services for Call Forward and Call Transfer	Allows you to prevent REFER messages for call transfers and redirect responses for call forwarding from being sent by Cisco Unified CME if a destination gateway does not support supplementary services. Supports disabling of supplementary services if all endpoints use SCCP or all endpoints use SIP.	
	Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode	Routes callers dialing 911 to the correct location.	Enhanced 911 Services, on page 687
	KPML	Allows Key Press Markup Language (KPML) to report SIP phone users' input digit by digit to Cisco Unified CME, which performs pattern recognition by matching a destination pattern to a dial peer as it collects the dialed digits.	
	Multi-Party Conferencing Enhancements	Provides the following enhancements: • Enhanced ad-hoc conferences are hardware-based and allow more than three parties. • Meet-me conferences consist of at least three parties dialing a meet-me conference number.	Conferencing, on page 1369
	Network Time Protocol		Network Parameters, on page 121

Version	Feature Name	Feature Description	Where Documented
		Allows SIP phones registered to a Cisco Unified CME router to synchronize to a Network Time Protocol (NTP) server, known as the clock master.	
	Out-of-Dialog REFER	Allows remote applications to establish calls by sending an out-of-dialog REFER (OOD-R) message to Cisco Unified CME without an initial INVITE. After the REFER message is sent, the remainder of the call setup is independent of the application and the media stream does not flow through the application.	Network Parameters, on page 121
	Presence with BLF Status	Allows presence to support BLF notification features for speed dial buttons and directory call lists for missed calls, placed calls, and received calls. SIP and SCCP phones that support BLF speed-dial and BLF call-list features can subscribe to status notification for internal and external directory numbers.	Presence Service, on page 875
	Restarting Phones	Allows SIP phones to quickly reset using the **restart** command. Phones contact the TFTP server for updated configuration information and re-register without contacting the DHCP server.	Reset and Restart Cisco Unified IP Phones, on page 397

Version	Feature Name	Feature Description	Where Documented
	Session Transport	Allows TCP to be used as the transport protocol for supported SIP phones connected to Cisco Unified CME. Previously, only UDP was supported.	
	SIP Dial Plans	Enables SIP phones to perform local digit collection and recognize dial patterns as user input is collected using dial plans. After a pattern is recognized, the SIP phone sends an INVITE message to Cisco Unified CME to initiate the call.	
	Softkeys	Allows you to customize the display and order of softkeys that appear on individual SIP phones during the connected, hold, idle, and seized call states.	Customize Softkeys, on page 925
	Translation Rules	Allows SIP phones in a Cisco Unified CME system to support translation rules with functionality similar to phones running SCCP. Translation rules can be applied to incoming calls for directory numbers on a SIP phone.	Dial Plans, on page 445
Cisco Unified CME 4.0(3)			

Version	Feature Name	Feature Description	Where Documented
4.0(3)	AMWI	Allows Cisco Unified IP Phone 7911 and Cisco Unified IP Phone 7931G to be configured to receive AMWI (Audible Message Line Indicator) and visual MWI notification from an external voice-messaging system.	Voice Mail Integration, on page 539
	Cisco Unified IP Phones	Adds support for the following phones: • Cisco Unified IP Phone 7906G • Cisco Unified IP Phone 7931G	Cisco Unified CME 4.0(3) Supported Firmware, Platforms, Memory, and Voice Products
	DSS	Introduces the DSS (Direct Station Select) feature that allows the phone user to press a single speed-dial line button to transfer an incoming call when the call is in the connected state. This feature is supported on all phones on which monitor line buttons for speed dial or speed-dial line buttons are configured.	Speed Dial, on page 965
	Extension Assigner	Allows installation technicians to assign extension numbers to phones without administrative access to Cisco Unified CME, typically during the installation of new phones or the replacement of broken phones.	Create Phone Configurations Using Extension Assigner, on page 347
	Fax Relay		Configure Fax Relay, on page 753

Version	Feature Name	Feature Description	Where Documented
		Introduces a SCCP-enhanced feature that adds support for Cisco Fax Relay and Super Group 3 (SG3) to G3 fax relay. The feature allows the fax stream between two SG3 fax machines to negotiate down to G3 speeds (less than 14.4 kbps) allowing SG3 fax machines to interoperate over fax relay with G3 fax machines.	
Cisco Unified CME 4.0(1)			

Version	Feature Name	Feature Description	Where Documented
4.0(1)	Call Forwarding	**Automatic call forwarding during night service—**Ephone-dns (extensions) can be designated to automatically forward their calls to a specified number during the time that night service is in effect. **Blocking call forwarding of local calls—**Forwarding of local (internal) calls from other Cisco Unified CME ephones can be blocked. External calls will continue to be forwarded as specified by the configuration for the ephone-dns. **Selective call forwarding—**Call forwarding for busy and no-answer ephone-dns can be applied selectively based on the number that a caller dials for a particular ephone-dn: the primary number, the secondary number, or either of those numbers expanded through the use of a dial-plan pattern.	

Version	Feature Name	Feature Description	Where Documented
	Call Park	**Call park blocked per ephone—**Individual ephones can be blocked from parking calls at call-park slots. **Call park redirect—**You can specify that calls use the H.450 or SIP Refer method of call forwarding or transfer to park calls and to pick up calls from park. **Dedicated call-park slots—**A private call-park slot can be configured for each ephone. **Direct pickup of parked call on monitored park slot —**A call that is parked on a monitored call-park slot can be picked up by pressing the assigned monitor button.	
	Call Pickup	**Directed call pickup disable—**The **no service directed-pickup** command globally disables directed call pickup and changes the action of the PickUp softkey to invoke local group pickup rather than directed call pickup.	Call Coverage Features, on page 1239
	Call Transfer		

Version	Feature Name	Feature Description	Where Documented
		Call transfer blocking—When call transfers to phones outside the Cisco Unified CME system have been globally enabled, you can block them for individual ephones. **Call transfer destination digits limited**—When call transfers to phones outside the Cisco Unified CME system have been globally enabled, you can limit the number of digits that can be dialed when transferring a call. **transfer-system command**—The command default has been changed from the **blind** keyword to the **full-consult** keyword, making H.450.2 consultative transfer the default method. **QSIG supplementary services support**—H.450 supplementary services features allow Cisco Unified CME phones to use QSIG to interwork with PBX phones. IP phones can use a PBX message center with proper MWI notifications.	
	Cisco Unified IP Phones		Cisco Unified CME 4.0 Supported Firmware, Platforms, Memory, And Voice Products

Version	Feature Name	Feature Description	Where Documented
		Adds support for the following phones: • Cisco Unified IP Phone 7911G • Cisco Unified IP Phone 7941G and 7941G-GE • Cisco Unified IP Phone 7961G and 7961G-GE No additional configuration is required for these phones. They are supported in the appropriate Cisco IOS commands.	
	Conferencing	**Drop last party or keep parties connected—**New options specify whether the last party that joined a conference can be dropped from the conference and whether the remaining two parties should be allowed to continue their connection after the conference initiator has left the conference. **Improved conference display—**A Cisco Unified IP phone that is connected to a three-way conference displays "Conference." No special configuration is required.	Conferencing, on page 1369

Version	Feature Name	Feature Description	Where Documented
	Feature Access Codes	**Feature Access Code (FAC) support—**The same FACs that are used by analog phones can be enabled for IP phones. In addition, standard FACs can be customized and aliases can be created to simplify the dialing of a FAC and any additional digits that are required to activate the feature.	Feature Access Codes, on page 757
	Headset Auto-Answer	**Headset auto-answer—**When the headset key on a phone is activated, lines on the phone that are specified for headset auto-answer will automatically connect to incoming calls after playing an alerting tone to notify the phone user of the incoming call. This feature is available on Cisco Unified IP Phones 7940G, 7960G, 7970G, and 7971G-GE.	Headset Auto Answer, on page 777

Version	Feature Name	Feature Description	Where Documented
	Hunt Groups		Call Coverage Features, on page 1239

Version	Feature Name	Feature Description	Where Documented
		Agent status control—Hunt group agents can put their phones in a not-ready state to temporarily suspend the receiving of hunt group calls by using the HLog softkey. A new FAC can toggle ready and not-ready state. **Automatic agent not-ready status—**The criterion for placing a hunt group agent into not-ready status (previously called automatic logout) was changed. If an agent does not answer the number of consecutive hunt-group calls that you specify in the **auto logout** command, the agent's ephone-dn is put into not-ready status (logged out) and will not receive further hunt group calls. **Call hold statistics—**New fields describing the length of time that calls spend in the hold state are in the statistical reports for Cisco Unified CME B-ACD applications. See the **show ephone-hunt statistics** command and the **hunt-group report url** command in Cisco Unified CME B-ACD and Tcl Call-Handling Applications. **Dynamic hunt group membership—**Agents can join or leave a hunt group using standard or custom FACs when	

Version	Feature Name	Feature Description	Where Documented
		wildcard slots are configured for hunt groups and the agents' ephone-dns are authorized to join hunt groups. **Change in hops command default—**The maximum number of hops allowed by a hunt group is automatically adjusted to reflect the dynamically changing number of members. **Enhanced display of ephone hunt-group information—**A text string can be added to provide information in configuration output and to display on IP phones when a hunt-group call is ringing or answered or when all hunt-group members are logged out. **Local call forwarding restriction in sequential ephone hunt groups—**In sequential ephone-hunt groups, local (internal) calls to the hunt group can be prevented from being forwarded beyond the first ephone-dn in the hunt group.	

Version	Feature Name	Feature Description	Where Documented
	Hunt Groups		Call Coverage Features, on page 1239

Version	Feature Name	Feature Description	Where Documented
		Longest-idle hunt group improvement—The **from-ring** command specifies that on-hook time stamps should be updated when a call rings an agent and when a call is answered by an agent. **Maximum number of agents—**The maximum number of agents per hunt group has increased from 10 to 20. No special configuration is required. **Maximum number of hunt groups—**The maximum number of hunt groups per Cisco Unified CME system has increased from 10 to 100. No special configuration is required. **No-answer timeout enhancements—**No-answer timeouts in ephone hunt groups can be set individually for each ephone-dn in the list. A maximum cumulative no-answer timeout can be also be set. **Restricting presentation of calls to idle or on-hook phones—**The presentation of hunt group calls can be restricted to hunt-group members on phones that are idle or on-hook. This enhancement considers all lines on the phone, both members of the hunt group and nonmembers, when restricting presentation of hunt group calls.	

Version	Feature Name	Feature Description	Where Documented
		Return to a secondary destination in an ephone hunt group after call park—Calls parked by hunt group agents can be returned to a different entry point in the hunt group. **Return to transferring party on no answer in an ephone hunt group—**A call that was transferred into a hunt group and was not answered can be returned to the party that transferred it to the hunt group instead of being sent to voice mail or another final destination.	
	Localization	**Multiple user locales and network locales—**Up to five user and network locales are supported. **User-defined user locales and network locales—** User-defined locales can be added for supported phones.	

Version	Feature Name	Feature Description	Where Documented
	Music on Hold	**Music on hold (MOH) for internal calls—**Internal callers (those making calls between extensions in the same Cisco Unified CME system) hear music when they are on hold or are being transferred. The **mulitcast moh** command must be used to enable the flow of packets to the subnet on which the phones are located. Internal extensions that are connected through an analog voice gateway or through a WAN (remote extensions) do not hear MOH on internal calls. The ability to disable multicast MOH per phone was introduced, using the **no multicast-moh** command in ephone or ephone-template configuration mode.	Music on Hold, on page 829

Version	Feature Name	Feature Description	Where Documented
	Overlaid Ephone-dns	**Overlaid ephone-dns—**The maximum number of overlaid ephone-dns per ephone button has increased from 10 to 25. No special configuration is required. **Overlaid ephone-dn call-waiting display—**The number of waiting calls that can be displayed for overlaid ephone-dns that have call waiting configured has been increased to six for the Cisco IP Phone 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G, and 7971G-GE. The overlaid ephone-dns must be configured on the phone using the **button** command and the **c** keyword. **Overlaid ephone-dn call overflow to other buttons—**One or more buttons can be dedicated to serve as expansion or overflow buttons for another button on the same Cisco Unified IP phone that has overlaid ephone-dns. A call to an overlay button that is busy with an active call will roll over to the next available expansion button.	Call Coverage Features, on page 1239
	Phone Support		

Version	Feature Name	Feature Description	Where Documented
		Cisco IP Communicator is a software-based application that appears on a user's computer monitor as a graphical, display-based IP phone with a color screen, a key pad, feature buttons, and softkeys. Cisco Unified CME supports Cisco IP Communicator 2.0 and later versions. **Remote teleworker phone**—Teleworkers can connect remote phones over a WAN and be directly supported by Cisco Unified CME.	
	Ring Tones	**Distinctive ringing**—An extension's ring patterns can be set to distinguish among internal, external, and feature calls.	Ringtones, on page 899
	Security	**Cisco Unified CME phone authentication** is a security infrastructure for providing secure Skinny Client Control Protocol (SCCP) signaling between Cisco Unified CME and IP phones.	Security, on page 581
	Softkeys		Customize Softkeys, on page 925

Version	Feature Name	Feature Description	Where Documented
		Feature blocking—The features associated with the following softkeys can be individually blocked per ephone: CFwdAll, Confrn, GpickUp, Park, PickUp, and Trnsfer. The softkey is not removed, but it does not function. **Softkey control for hold state**—The softkeys that are available while a call is on hold can be modified. The NewCall and Resume softkeys are normally available when a phone has a call on hold, but a template can be applied to the phone to remove these softkeys.	
	Speed Dial	**Bulk-loading of speed-dial numbers**—Text files with lists of speed-dial numbers can be loaded into system flash or a URL. The files can hold up to 10,000 numbers and can be applied to all ephones or to specific ephones.	Speed Dial, on page 965

Version	Feature Name	Feature Description	Where Documented
	System-Level Parameters		

Version	Feature Name	Feature Description	Where Documented
		Disabling automatic phone registration—Normally, Cisco Unified CME allocates an ephone slot to any ephone that connects to the system. To prevent unauthorized registrations, the **no auto-reg-ephone** command prevents any ephone from registering with Cisco Unified CME if its MAC address is not explicitly listed in the configuration. **External storage of configuration files and per-phone configuration files**—Phone configuration files can be stored on an external TFTP server to offload the TFTP server function of the Cisco Unified CME router. This additional storage space permits the use of per-phone configuration files, which can be used to specify different user locales and network locales for phones. **Failover to Redundant Router**—Sites can be set up with a primary and secondary Cisco Unified CME router to provide redundant Cisco Unified CME capability. Phones automatically register at the secondary router if the primary router fails and later rehome to the primary router when it is	

Version	Feature Name	Feature Description	Where Documented
		operational again.	
	Templates	**Maximum number of ephone templates—**The maximum number of ephone templates that can be defined has increased from 5 to 20. No special configuration is required. **New commands available for ephone templates—**Ephone templates were previously introduced to allow system administrators to control the display of softkeys in various call states on individual ephones. Their role has been expanded to allow you to define a set of ephone parameter values that can be assigned to one or more phones in a single step. **Ephone-dn templates—**Ephone-dn templates are introduced to allow administrators to easily apply sets of configured parameters to individual ephone-dns. Up to 15 ephone-dn templates can be defined.	Templates, on page 1427
	Video Support		Video Support, on page 987

Version	Feature Name	Feature Description	Where Documented
		Video support for SCCP-based endpoints—This feature adds video support to allow you to pass a video stream with a voice call between video-capable SCCP endpoints and between SCCP and H.323 endpoints. Through the Cisco Unified CME router, the video-capable endpoints can communicate with each other locally to a remote H.323 endpoint through a gateway or through an H.323 network.	
	Voice Mail		Voice Mail Integration, on page 539

Version	Feature Name	Feature Description	Where Documented
		Line-selectable MWI—Previously, the message-waiting indication (MWI) lamp on a phone could only indicate when messages were waiting for the primary number on a phone. Now, any phone line can be designated during configuration. **Mailbox selection policy for voice-mail servers—**A policy can be set for selecting the mailbox to use for calls that are diverted one or more times within a Cisco Unified CME system before being sent to a Cisco Unity Express, Cisco Unity, or PBX voice-mail pilot number. **Prefix option for SIP unsolicited MWI Notify messages—**Central voice-message servers that provide mailboxes for multiple Cisco Unified CME sites may use site codes or prefixes to distinguish among similarly numbered ranges of extensions at different sites. You can specify the prefix for your site so that central mailbox numbers are correctly converted to your extension numbers.	
	XML Interface		Configure XML API, on page 1609

Version	Feature Name	Feature Description	Where Documented
		XML interface enhancements—An eXtensible Markup Language (XML) application program interface (API) is provided to supply data from Cisco Unified CME to management software. In Cisco Unified CME 4.0 and later versions, all Cisco Unified CME features have XML support.	

• Obtaining Documentation, Obtaining Support, and Security Guidelines, page 65

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

DISCLAIMER: The use of monitoring, recording, or listening devices to eavesdrop, monitor, retrieve, or record phone conversations or other sound activities, whether or not contemporaneous with transmission, may be illegal in certain circumstances under federal, state and/or local laws. Legal advice should be sought prior to implementing any practice that monitors or records any phone conversation. Some laws require some form of notification to all parties to a phone conversation, such as by using a beep tone or other notification method or requiring the consent of all parties to the phone conversation, prior to monitoring or recording the phone conversation. Some of these laws incorporate strict penalties. In cases where local laws require a periodic beep while a conversation is being recorded, the Cisco Unity Express voice-mail system provides a user with the option of activating "the beep." Prior to activating the Cisco Unity Express live record function, check the laws of all applicable jurisdictions. This is not legal advice and should not take the place of obtaining legal advice from a lawyer. IN ADDITION TO THE GENERAL DISCLAIMER THAT ACCOMPANIES THIS CISCO UNITY EXPRESS PRODUCT, CISCO ADDITIONALLY DISCLAIMS ANY AND ALL LIABILITY, BOTH CIVIL AND CRIMINAL, AND ASSUMES NO RESPONSIBILITY FOR THE UNAUTHORIZED AND/OR ILLEGAL USE OF THIS CISCO UNITY EXPRESS PRODUCT. THIS DISCLAIMER OF LIABILITY INCLUDES, BUT IS NOT NECESSARILY LIMITED TO, THE UNAUTHORIZED AND/OR ILLEGAL RECORDING AND MONITORING OF TELEPHONE CONVERSATIONS IN VIOLATION OF APPLICABLE FEDERAL, STATE AND/OR LOCAL LAWS.</p>

CHAPTER 2

Cisco Unified CME Overview

Important Information about Cisco IOS XE 16 Denali

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

For migration information related to the Cisco IOS XE 16, see Cisco IOS XE Denali 16.2 Migration Guide for Access and Edge Routers.

Introduction

Note The Cisco Unified Communications Manager Express System Administrator Guide refers to a phone with SIP firmware as SIP Phone, SIP IP Phone, or Cisco Unified SIP IP phone. A phone with SCCP firmware is referred as SCCP Phone, SCCP IP Phone, or Cisco Unified SCCP IP phone.

Cisco Unified Communications Manager Express (formerly known as Cisco Unified CallManager Express) is a call-processing application in Cisco IOS software that enables Cisco routers to deliver key-system or hybrid PBX functionality for enterprise branch offices or small businesses.

Cisco Unified CME is a feature-rich entry-level IP telephony solution that is integrated directly into Cisco IOS software. Cisco Unified CME allows small business customers and autonomous small enterprise branch offices to deploy voice, data, and IP telephony on a single platform for small offices, thereby streamlining operations and lowering network costs.

Cisco Unified CME is ideal for customers who have data connectivity requirements and also have a need for a telephony solution in the same office. Whether offered through a service provider's managed services offering or purchased directly by a corporation, Cisco Unified CME offers most of the core telephony features required in the small office, and also many advanced features not available with traditional telephony solutions. The ability to deliver IP telephony and data routing by using a single converged solution allows customers to optimize their operations and maintenance costs, resulting in a very cost-effective solution that meets office needs.

A Cisco Unified CME system is extremely flexible because it is modular. A Cisco Unified CME system consists of a router that serves as a gateway and one or more VLANs that connect IP phones and phone devices to the router.

Figure 1: Cisco Unified CME for the Small- and Medium-Size Office, on page 68 shows a typical deployment of Cisco Unified CME with several phones and devices connected to it. The Cisco Unified CME router is connected to the public switched telephone network (PSTN). The router can also connect to a gatekeeper and a RADIUS billing server in the same network.

Figure 1: Cisco Unified CME for the Small- and Medium-Size Office

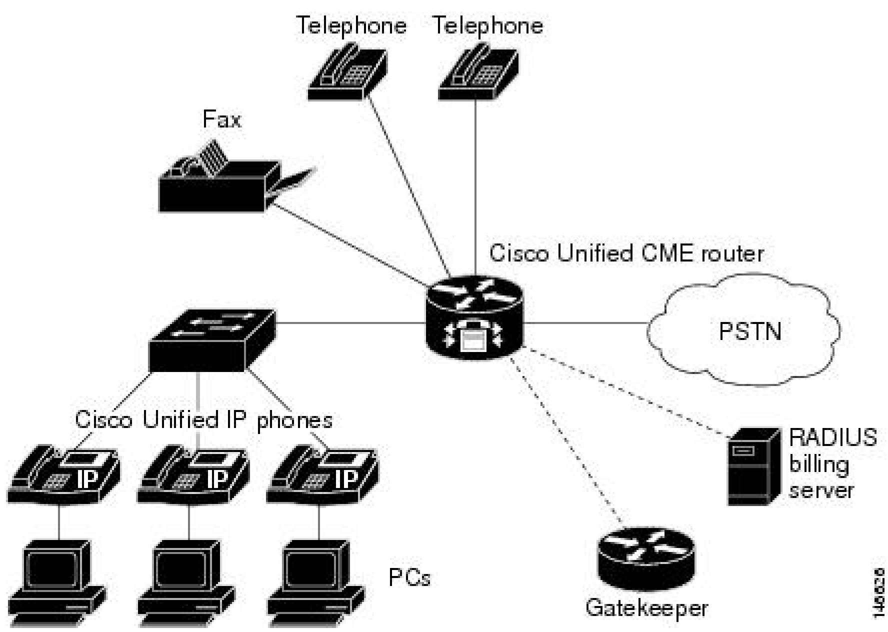
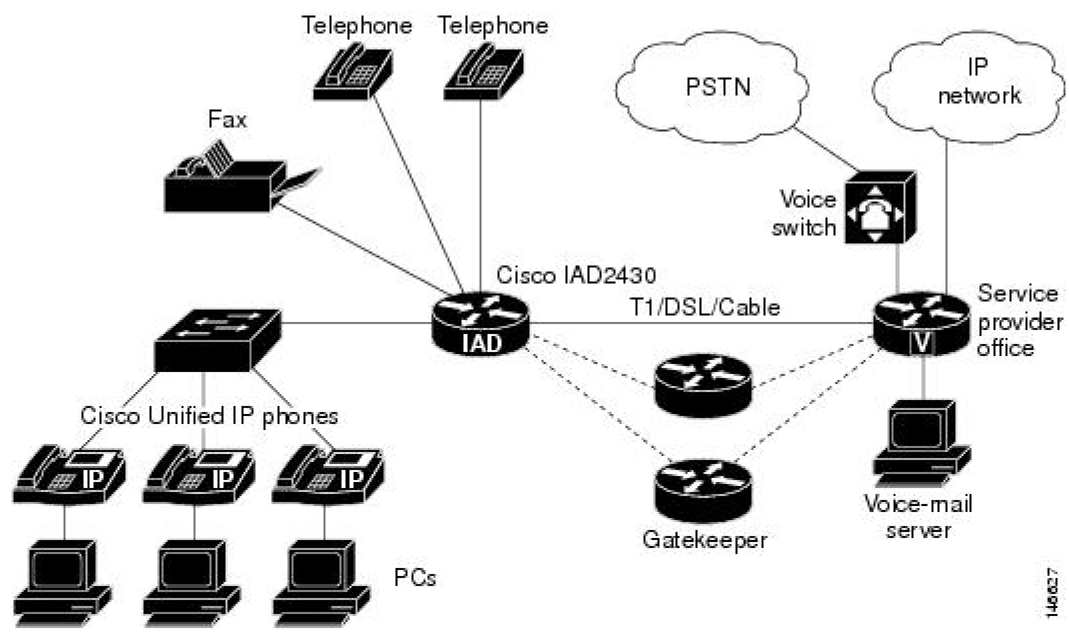


Figure 2: Cisco Unified CME for Service Providers, on page 69 shows a branch office with several Cisco Unified IP phones connected to a Cisco IAD2430 series router with Cisco Unified CME. The

Cisco IAD2430 router is connected to a multiservice router at a service provider office, which provides connection to the WAN and PSTN.

Figure 2: Cisco Unified CME for Service Providers



A Cisco Unified CME system uses the following basic building blocks:

- Ephone or voice register pool—A software concept that usually represents a physical telephone, although it is also used to represent a port that connects to a voice-mail system, and provides the ability to configure a physical phone using Cisco IOS software. Each phone can have multiple extensions associated with it and a single extension can be assigned to multiple phones. Maximum number of ephones and voice register pools supported in a Cisco Unified CME system is equal to the maximum number of physical phones that can be connected to the system.
- Directory number—A software concept that represents the line that connects a voice channel to a phone. A directory number represents a virtual voice port in the Cisco Unified CME system, so the maximum number of directory numbers supported in Cisco Unified CME is the maximum number of simultaneous call connections that can occur. This concept is different from the maximum number of physical lines in a traditional telephony system.

Licenses

You must purchase a base Cisco Unified CME feature license and phone user licenses that entitle you to use Cisco Unified CME. In Cisco Unified CME Release 11, you should purchase:

Cisco Unified CME Permanent License

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

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

Collaboration Professional Suite License

Collaboration Professional is a new suite of licenses. The Collaboration Professional Suite can be purchased either as a permanent license or an RTU license.

Collaboration Professional Suite Permanent License —When you purchase the Collaboration Professional Suite license, by default, the Cisco Unified CME licenses are delivered as part of the Collaboration Professional Suite. You do not have to separately install and activate the Cisco Unified CME license. The Collaboration Professional Suite permanent license is available in the form of an XML file. You should get the XML file and load it in the flash memory of the device. To install the permanent license from the command prompt, use the **license install flash:lic_name** command.

Collaboration Professional Suite RTU License—When you purchase the Collaboration Professional Suite RTU license, you do not have to go through the Evaluation Right to Use process. However, you have to go through the RTU licensing process for using the Cisco Unified CME features. To install the Collaboration Professional Suite RTU license from the command prompt, use the **license install flash0:colla_pro** command. To activate the license, use the **license boot module c2951 technology-package collabProSuitek9** command.

Cisco Smart License

From Release 11.7 onwards, Cisco Unified CME supports Smart Licensing, apart from the existing CSL licensing model. Smart Licensing is supported only on Cisco 4000 Series Integrated Services Router. Depending on the technology package available on the router, licenses such as UCK9 and Security are supported using Smart Licensing.

Note Cisco Smart Software Manager satellite which is a component of Cisco Smart Licensing is not supported for Unified CME.

The Smart Licensing feature is a software based licensing model that gives you visibility into license ownership and consumption. The Smart Licensing model consists of a web interface named Cisco Smart Software Manager (CSSM). CSSM is a central license repository that manages licenses across all Cisco products that you own, including Unified CME. Your access to the CSSM account is authenticated using valid Cisco credentials.

You can use the CSSM Smart Account to generate valid tokens IDs. The token IDs are used to register the Unified CME device with your CSSM Smart Account. Once the token is generated, it can be used to register many other product instances in your network.

On the Unified CME router, you need to ensure that the call home feature is not disabled. Also, Smart Licensing feature should be enabled at the router using the CLI command **license smart enable**. Use the **no** form of the command to disable smart licensing. For more information on configuring Smart Licensing in your router, see Software Activation Configuration Guide, Cisco IOS Release 15M&T. Once the smart license is enabled and the router is not yet registered with CSSM, the device enters an evaluation period of 90 days.

You can register the router to CSSM with the token ID. To register the device (Unified CME router) with CSSM, use the CLI command **license smart register idtoken**. For information on registering the device with CSSM, see Software Activation Configuration Guide.

Upon successful registration, Unified CME is in Registered status. Then, Unified CME sends an authorization request for all the phones configured. Based on the licenses in the Smart Account, CSSM responds with one of the defined statuses such as Authorized (using less than it has licenses for) or Out-of-Compliance (using more than it has licenses for).

The CSSM assigns licenses that are available in your CSSM account to the phones configured across the routers. Unified CME supports only one license entitlement to validate phones configured on Unified CME.

- CME_EP—This license type supports all phones configured on Unified CME.

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

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

Note If the router does not communicate with CSSM for a period of 90 days, the license authorization expires.

The license count is evaluated for the number of phones configured across the routers. The CSSM Licenses page reflects the total license count usage. The total number of licenses available for a type of license (Quantity), number of licenses currently use (In Use), and the number of unused or over-used licenses (Surplus/Shortage).

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

Once a new phone is configured on a Unified CME registered with CSSM, a timer is initiated to report the phone configuration to CSSM. A new phone configuration is reported only at the end of the time set in the timer (3 minutes). Hence, the Smart Agent reports all the new configurations created within the time period defined using the preset timer. The CSSM increments the license usage count based on the report sent by Smart Agent. If the number of phones configured exceeds the license limit, then CSSM generates an alert in the user account. When a phone configuration is removed, the license usage count is decremented.

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

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

Registration:
 Status: REGISTERED
 Smart Account: Call-Manager-Express
 Virtual Account: CME Application
 Export-Controlled Functionality: Not Allowed
 Last Renewal Attempt: None
 Next Renewal Attempt: Oct 07 12:08:10 2016 UTC
```

```
License Authorization:
 Status: AUTHORIZED
 Last Communication Attempt: SUCCESS
 Next Communication Attempt: May 13 07:11:48 2016 UTC

License Usage:

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

Licensing Modes

From Unified CME 11.7 onwards, both CSL and Smart Licensing modes are supported. That is, customers can continue with CSL by not enabling Smart Licensing. Alternatively, they can enable Smart Licensing and decide later to go back to CSL by disabling Smart Licensing with the **no license smart enable** command. When you switch to CSL from the Smart Licensing mode, you need to ensure that the End User License Agreement (EULA) is signed. CSL is not supported unless the EULA is signed. Use the CLI command **license accept end user agreement** in global configuration mode to configure EULA.

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

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

Restrictions

- For the Cisco Unified CME license, the UCK9 technology package must be available if the Collaboration Professional Suite package is not installed.
- UCK9 is a prerequisite for Cisco Unified CME Release 11.

Note As compared to Unified CME Release 10.5 and prior, all the future releases of Unified CME displays the CME-SRST license state as **Active, Not in Use**. This is applicable when Unified CME is removed from the router (configure **no telephony-service** and **no voice register global** to remove Unified CME from the router).

To activate the Cisco Unified CME feature license, see Activating CME-SRST Feature License.

Note To support H.323 call transfers and forwards to network devices that do not support the H.450 standard, such as Cisco Unified Communications Manager, a tandem gateway is required in the network. The tandem gateway must be running Cisco IOS Release 12.3(7)T or a later release and requires the Integrated Voice and Video Services feature license (FL-GK-NEW-xxx), which includes the H.323 gatekeeper, IP-to-IP gateway, and H.450 tandem functionality.

PBX or Keyswitch

When setting up a Cisco Unified CME system, you need to decide if call handling should be similar to that of a PBX, similar to that of a keyswitch, or a hybrid of both. Cisco Unified CME provides significant flexibility in this area, but you must have a clear understanding of the model that you choose.

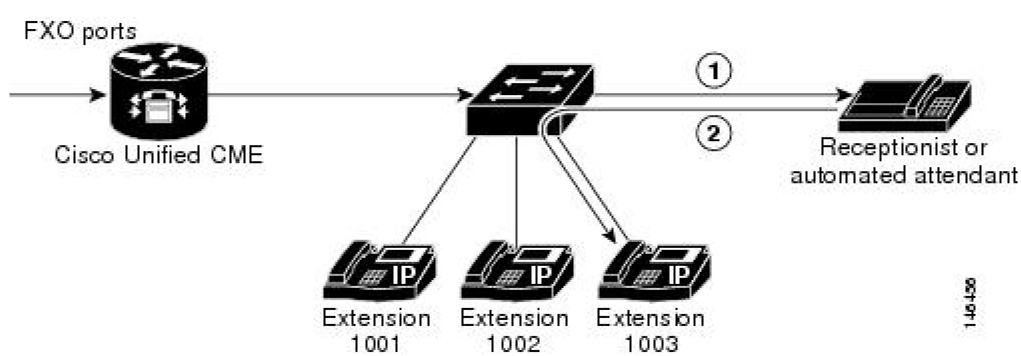
PBX Model

The simplest model is the PBX model, in which most of the IP phones in your system have a single unique extension number. Incoming PSTN calls are routed to a receptionist at an attendant console or to an automated attendant. Phone users may be in separate offices or be geographically separated and therefore often use the telephone to contact each other.

For this model, we recommend that you configure directory numbers as dual-lines so that each button that appears on an IP phone can handle two concurrent calls. The phone user toggles between calls using the blue navigation button on the phone. Dual-line directory numbers enable your configuration to support call waiting, call transfer with consultation, and three-party conferencing (G.711 only).

Figure 3: Incoming Call Using PBX Model, on page 73 shows a PSTN call that is received at the Cisco Unified CME router, which sends it to the designated receptionist or automated attendant (1), which then routes it to the requested extension (2).

Figure 3: Incoming Call Using PBX Model



For configuration information, see Configure Phones for a PBX System, on page 253.

Keyswitch Model

In a keyswitch system, you can set up most of your phones to have a nearly identical configuration, in which each phone is able to answer any incoming PSTN call on any line. Phone users are generally close to each other and seldom need to use the telephone to contact each other.

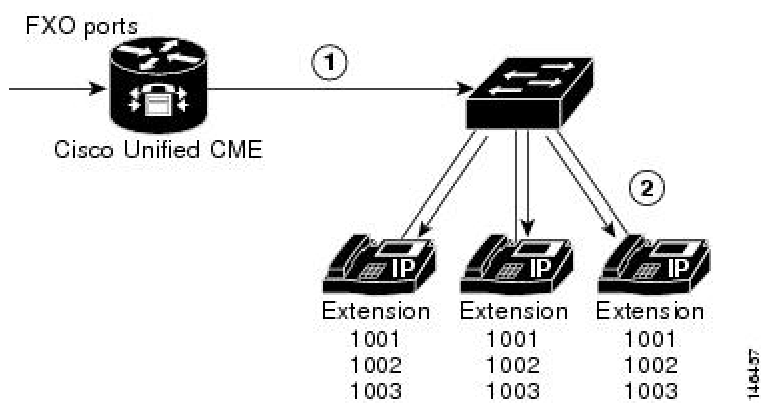
For example, a 3x3 keyswitch system has three PSTN lines shared across three telephones, such that all three PSTN lines appear on each of the three telephones. This permits an incoming call on any PSTN line to be directly answered by any telephone—without the aid of a receptionist, an auto-attendant service, or the use of (expensive) DID lines. Also, the lines act as shared lines—a call can be put on hold on one phone and resumed on another phone without invoking call transfer.

In the keyswitch model, the same directory numbers are assigned to all IP phones. When an incoming call arrives, it rings all available IP phones. When multiple calls are present within the system at the same time, each individual call (ringing or waiting on hold) is visible and can be directly selected by pressing the corresponding line button on an IP phone. In this model, calls can be moved between phones simply by putting the call on hold at one phone and selecting the call using the line button on another phone. In a keyswitch model, the dual-line option is rarely appropriate because the PSTN lines to which the directory numbers correspond do not themselves support dual-line configuration. Using the dual-line option also makes configuration of call-coverage (hunting) behaviors more complex.

You configure the keyswitch model by creating a set of directory numbers that correspond one-to-one with your PSTN lines. Then you configure your PSTN ports to route incoming calls to those ephone-dns. The maximum number of PSTN lines that you can assign in this model can be limited by the number of available buttons on your IP phones. If so, the overlay option may be useful for extending the number of lines that can be accessed by a phone.

Figure 4: Incoming PSTN Call Using Keyswitch Model, on page 74 shows an incoming call from the PSTN (1), which is routed to extension 1001 on all three phones (2).

Figure 4: Incoming PSTN Call Using Keyswitch Model



For configuration information, see Configure Phones for a Key System, on page 282.

Hybrid Model

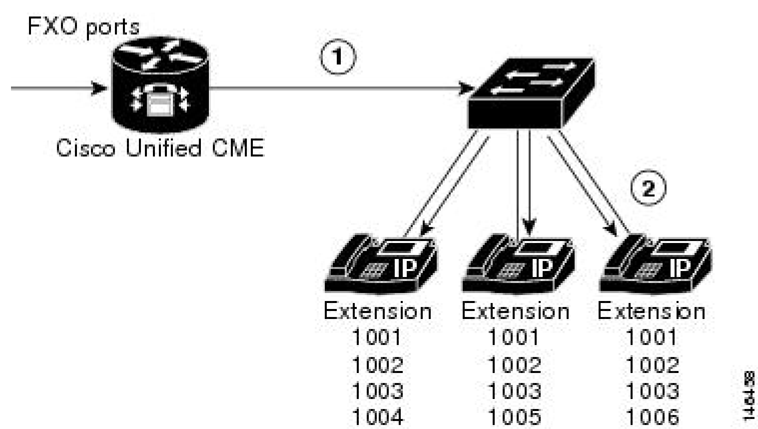
PBX and keyswitch configurations can be mixed on the same IP phone and can include both unique per-phone extensions for PBX-style calling and shared lines for keyswitch-style call operations. Single-line and dual-line directory numbers can be combined on the same phone.

In the simplest keyswitch deployments, individual telephones do not have private extension numbers. Where key system telephones do have individual lines, the lines are sometimes referred to as intercoms rather than as extensions. The term “Intercom” is derived from “internal communication;” there is no assumption of the common “intercom press-to-talk” behavior of auto dial or auto answer in this context, although those options may exist.

For key systems that have individual intercom (extension) lines, PSTN calls can usually be transferred from one key system phone to another using the intercom (extension) line. When Call Transfer is invoked in the context of a connected PSTN line, the outbound consultation call is usually placed from the transferrer phone to the transfer-to phone using one of the phone’s intercom (extension) line buttons. When the transferred call is connected to the transfer-to phone and the transfer is committed (the transferrer hangs up), the intercom lines on both phones are normally released and the transfer-to call continues in the context of the original PSTN line button (all PSTN lines are directly available on all phones). The transferred call can be put on hold (on the PSTN line button) and then subsequently resumed from another phone that shares that PSTN line.

For example, you can design a 3x3 keyswitch system as shown in Figure 4: Incoming PSTN Call Using Keyswitch Model, on page 74 and then add another, unique extension on each phone (Figure 5: Incoming PSTN Call Using Hybrid PBX-Keyswitch Model, on page 75). This setup will allow each phone to have a “private” line to use to call the other phones or to make outgoing calls.

Figure 5: Incoming PSTN Call Using Hybrid PBX-Keyswitch Model



Call Detail Records

The accounting process collects accounting data for each call leg created on the Cisco voice gateway. You can use this information for post-processing activities such as generating billing records and network analysis. Voice gateways capture accounting data in the form of call detail records (CDRs) containing attributes defined by Cisco. The gateway can send CDRs to a RADIUS server, syslog server, or to a file in .csv format for storing to flash or an FTP server. For information about generating CDRs, see CDR Accounting for Cisco IOS Voice Gateways.

Additional References

The following section provides references related to Cisco Unified CME.

Table 2: Related Documents for Unified CME

Related Topic	Document Title
Cisco Unified CME configuration	Cisco Unified CME Command Reference Cisco Unified CME Documentation Roadmap
Cisco IOS commands	Cisco IOS Voice Command Reference Cisco IOS Software Releases 12.4T Command References
Cisco IOS configuration	Cisco IOS Voice Configuration Library Cisco IOS Software Releases 12.4T Configuration Guides
Cisco IOS voice troubleshooting	Cisco IOS Voice Troubleshooting and Monitoring Guide
Dial peers, DID, and other dialing issues	Dial Peer Configuration on Voice Gateway Routers Understanding One Stage and Two Stage Dialing (technical note) Understanding How Inbound and Outbound Dial Peers Are Matched on Cisco IOS Platforms (technical note) Using IOS Translation Rules - Creating Scalable Dial Plans for VoIP Networks (sample configuration)
Dynamic Host Configuration Protocol (DHCP)	"DHCP" section of the Cisco IOS IP Addressing Services Configuration Guide
Fax and modem configurations	Cisco Fax Services over IP Application Guide
FXS ports	**FXS Ports in SCCP Mode on Cisco VG 224 Analog Phone Gateway** "Configuring Analog Voice Ports" section of the Cisco IOS Voice Port Configuration Guide **FXS Ports in SCCP Mode on Cisco VG 224 Analog Phone Gateway** SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways Cisco VG 224 Analog Phone Gateway data sheet

Related Topic	Document Title
H.323	Cisco IOS H.323 Configuration Guide
Network Time Protocol (NTP)	"Performing Basic System Management" chapter of Cisco IOS Network Management Configuration Guide
Phone documentation for Cisco Unified CME	User Documentation for Cisco Unified IP Phones
Public key infrastructure (PKI)	"Part 5: Implementing and Managing a PKI" in the Cisco IOS Security Configuration Guide
SIP	Cisco IOS SIP Configuration Guide
TAPI and TSP documentation	Cisco Unified CME programming Guides
Tcl IVR and VoiceXML	Cisco IOS Tcl IVR and VoiceXML Application Guide - 12.3(14)T and later Cisco Voice XML Programmer's Guide
VLAN class-of-service (COS) marking	Enterprise QoS Solution Reference Network Design Guide
Voice-mail integration	Cisco Unified CallManager Express 3.0 Integration Guide for Cisco Unity 4.0 Integrating Cisco CallManager Express with Cisco Unity Express
Call detail records (CDRs)	CDR Accounting for Cisco IOS Voice Gateways
XML	XML Provisioning Guide for Cisco CME/SRST Cisco IP Phone Services Application Development Notes

Management Information Base

MIBs	MIBs Link
CISCO-CCME-MIB MIB CISCO-VOICE-DIAL-CONTROL-MIB	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

CHAPTER 3

Before You Begin

Prerequisites for Configuring Cisco Unified CME

- Base Cisco Unified CME feature license and phone user licenses that entitle you to use Cisco Unified CME are purchased.

Note To support H.323 call transfers and forwards to network devices that do not support the H.450 standard, such as Cisco Unified Communications Manager, a tandem gateway is required in the network. The tandem gateway must be running Cisco IOS release 12.3(7)T or a later release and requires the Integrated Voice and Video Services feature license (FL-GK-NEW-xxx), which includes H.323 gatekeeper, IP-to-IP gateway, and H.450 tandem functionality.

- Your IP network is operational and you can access Cisco web.
- You have a valid Cisco.com account.
- You have access to a TFTP server for downloading files.

- Cisco router with all recommended services hardware for Cisco Unified CME is installed. For installation information, see Install Cisco Voice Services Hardware, on page 87.
- Recommended Cisco IOS IP Voice or higher image is downloaded to flash memory in the router.
    - To determine which Cisco IOS software release supports the recommended Cisco Unified CME version, see Cisco Unified CME and Cisco IOS Software Compatibility Matrix.
    - For a list of features for each Cisco IOS Software release, see Feature Navigator.
    - For installation information, see Install Cisco IOS Software, on page 89.
- VoIP networking must be operational. For quality and security purposes, we recommend separate virtual LANs (VLANs) for data and voice. The IP network assigned to each VLAN should be large enough to support addresses for all nodes on that VLAN. Cisco Unified CME phones receive their IP addresses from the voice network, whereas all other nodes such as PCs, servers, and printers receive their IP addresses from the data network. For configuration information, see Configure VLANs on a Cisco Switch, on page 90.

Restrictions for Configuring Cisco Unified CME

- Cisco Unified CME cannot register as a member of a Cisco Unified Communications Manager cluster.
- For conferencing and music on hold (MOH) support with G.729, hardware digital signal processors (DSPs) are required for transcoding G.729 between G.711.
- After a three-way conference is established, a participant cannot use call transfer to join the remaining conference participants to a different number.
- Cisco Unified CME does not support the following:
    - CiscoWorks IP Telephony Environment Monitor (ITEM)
    - Element Management System (EMS) integration
    - Media Gateway Control Protocol (MGCP) on-net calls
    - Java Telephony Application Programming Interface (JTAPI) applications, such as the Cisco IP Softphone, Cisco Unified Communications Manager Auto Attendant, or Cisco Personal Assistant
    - Telephony Application Programming Interface (TAPI)

      Cisco Unified CME implements only a small subset of TAPI functionality. It supports operation of multiple independent clients (for example, one client per phone line), but not full support for multiple-user or multiple-call handling, which is required for complex features such as automatic call distribution (ACD) and Cisco Unified Contact Center (formerly Cisco IPCC). Also, this TAPI version does not have direct media- and voice-handling capabilities.

Information About Planning Your Configuration

System Design

Traditional telephony systems are based on physical connections and are therefore limited in the types of phone services that they can offer. Because phone configurations and directory numbers in a Cisco Unified CME system are software entities and because the audio stream is packet-based, an almost limitless number of combinations of phone numbers, lines, and phones can be planned and implemented.

Cisco Unified CME systems can be designed in many ways. The key is to determine the total number of simultaneous calls you want to handle at your site and at each phone at your site, and how many different directory numbers and phones you want to have. Even a Cisco Unified CME system has its limits, however. Consider the following factors in your system design:

- Maximum number of phones—This number corresponds to the maximum number of devices that can be attached. The maximum is platform- and version-dependent. To find the maximum for your platform and version, see Cisco CME Supported Firmware, Platforms, Memory, and Voice Products.
- Maximum number of directory numbers—This number corresponds to the maximum number of simultaneous call connections that can occur. The maximum is platform- and version-dependent. To find the maximum for your platform and version, see Cisco CME Supported Firmware, Platforms, Memory, and Voice Products.
- Telephone number scheme—Your numbering plan may restrict the range of telephone numbers or extension numbers that you can use. For example, if you have DID, the PSTN may assign you a certain series of numbers.
- Maximum number of buttons per phone—You may be limited by the number of buttons and phones that your site can use. For example, you may have two people with six-button phones to answer 20 different telephone numbers.

The flexibility of a Cisco Unified CME system is due largely to the different types of directory numbers (DNs) that you can assign to phones in your system. By understanding types of DNs and considering how they can be combined, you can create the complete call coverage that your business requires. For more information about DNs, see Configuring Phones to Make Basic Calls, on page 223.

After setting up the DNs and phones that you need, you can add optional Cisco Unified CME features to create a telephony environment that enhances your business objectives. Cisco Unified CME systems are able to integrate with the PSTN and with your business requirements to allow you to continue using your existing number plans, dialing schemes, and call coverage patterns.

When creating number plans, dialing schemes, and call coverage patterns in Cisco Unified CME, there are several factors that you must consider:

- Is there an existing PBX or Key System that you are replacing and want to emulate?
- Number of phones and phone users to be supported?
- Do you want to use single-line or dual-line DNs?
- What protocols does your voice network support?
- Which call transfer and forwarding methods must be supported?

- What existing or preferred billing method do you want to use for transferred and forwarded calls?
- Do you need to optimize network bandwidth or minimize voice delay?

Because these factors can limit your choices for some of the configuration decisions that you will make when you create of a dialing plan, see the Cisco Unified Communications Manager Express Solution Reference Network Design Guide to help you understand the effect these factors have on your Cisco Unified CME implementation.

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Survivable Remote Site Telephony (Cisco Unified SRST), Cisco Unified Border Element, Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports—By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)—Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports—If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060—If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration—If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication—If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers—Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on Cisco Unified CME, Cisco Unified SRST, and Cisco Unified Border Element. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns—Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.

- Translation rules—Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts—Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation—Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)—If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see Cisco IOS Unified Communications Toll Fraud Prevention and Configure Toll Fraud Prevention, on page 513.

Cisco Unified CME Workflow

Table 3: Workflow for Creating or Modifying Basic Telephony Configuration, on page 83 lists the tasks for installing and configuring Cisco Unified CME and for modifying the configuration, in the order in which the tasks are to be performed and including links to modules in this guide that support each task.

Note Not all tasks are required for all Cisco Unified CME systems, depending on software version and on whether it is a new Cisco Unified CME, an existing Cisco router that is being upgraded to support Cisco Unified CME, or an existing Cisco Unified CME that is being upgraded or modified for new features or to add or remove phones.

Table 3: Workflow for Creating or Modifying Basic Telephony Configuration

Task	Cisco Unified CME Configuration		
	New	Modify	Documentation
Install Cisco router and all recommended services hardware for Cisco Unified CME.	Required	Optional	Install Cisco Voice Services Hardware, on page 87
Download recommended Cisco IOS IP Voice or higher image to flash memory in the router.	Optional	Optional	Install Cisco IOS Software, on page 89

Task	Cisco Unified CME Configuration		
	New	Modify	Documentation
Download recommended Cisco Unified CME software including phone firmware and GUI files.	Optional	Optional	Install and Upgrade Cisco Unified CME Software, on page 101
Configure separate virtual LANs (VLANS) for data and voice on the port switch.	Required	—	Network Assistant, on page 90 or Cisco IOS Commands, on page 91 or Internal Cisco Ethernet Switching Module, on page 94
• Enable calls in your VoIP network. • Define DHCP. • Set Network Time Protocol (NTP). • Configure DTMF Relay for H.323 networks in multisite installations. • Configure SIP trunk support. • Change the TFTP address on a DHCP server • Enable OOD-R.	Required	Optional	Network Parameters, on page 121

Task	Cisco Unified CME Configuration		
	New	Modify	Documentation
• Configure Bulk Registration. • Set up Cisco Unified CME. • Set date and time parameters. • Block Automatic Registration. • Define alternate location and type of configuration files. • Change defaults for Time Outs. • Configure a redundant router.	Required	Optional	System-Level Parameters, on page 149
• Create directory numbers and assigning directory numbers to phones. • Create phone configurations using Extension Assigner. • Generate configuration files for phones. • Reset or restart phones.	Required	Optional	Configure Phones to Make Basic Call, on page 315
Connect to PSTN.	Required	—	Dial Plans, on page 445
Install system- and user-defined files for localization of phones.	Optional	Optional	Localization Support, on page 407

Table 4: Workflow for Adding Features in Cisco Unified CME, on page 86 contains a list of tasks for adding commonly configured features in Cisco Unified CME and the module in which they appear in this guide. For a detailed list of features, with links to corresponding information in this guide, see Cisco Unified CME Features Roadmap, on page 1.

Table 4: Workflow for Adding Features in Cisco Unified CME

Task	Documentation
Configure transcoding to support conferencing, call transferring and forwarding, MOH, and Cisco Unity Express.	Transcoding Resources, on page 473
Enable the graphical user interface in Cisco Unified CME.	Graphical User Interface, on page 523
Configure support for voice mail.	Voice Mail Integration, on page 539
Configure interoperability with Cisco Unified CCX.	Interoperability with Cisco Unified CCX, on page 1495
Configure authentication support.	Security, on page 581
Add features. • Call Blocking • Call-Coverage Features, including: ◦ Call Hunt ◦ Call Pickup ◦ Call Waiting ◦ Callback Busy Subscriber ◦ Hunt Groups ◦ Night Service ◦ Overlaid Ephone-dns • Call Park • Call Transfer and Forwarding • Caller ID Blocking • Conferencing • Intercom Lines • Music on Hold (MOH) • Paging	• Automatic Line Selection, on page 1041 • Call Blocking, on page 1061 • Call Coverage Features, on page 1239 • Call Park, on page 1081 • Call Transfer and Forward, on page 1147 • Caller ID Blocking, on page 1363 • Conferencing, on page 1369 • Directory Services, on page 659 • Do Not Disturb, on page 679 • Extension Mobility, on page 725 • Feature Access Codes, on page 757 • Headset Auto Answer, on page 777 • Intercom Lines, on page 783 • Loopback Call Routing, on page 797 • Music on Hold, on page 829 • Paging, on page 857 • Presence Service, on page 875 • Ringtones, on page 899 • Customize Softkeys, on page 925 • Speed Dial, on page 965

Task	Documentation
Configure phone options, including: • Customized Background Images for Cisco Unified IP Phone 7970 • Fixed Line/Feature Buttons for Cisco Unified IP Phone 7931G • Header Bar Display • PC Port Disable • Phone Labels • Programmable vendorConfig Parameters • System Message Display • URL Provisioning for Feature Buttons	Modify Cisco Unified IP Phone Options, on page 1437
Configure video support.	Video Support, on page 987
Configure Cisco Unified CME as SRST Fallback.	SRST Fallback Mode, on page 1539

Install Cisco Voice Services Hardware

Note Cisco routers are normally shipped with Cisco voice services hardware and other optional equipment that you ordered already installed. In the event that the hardware is not installed or you are upgrading your existing Cisco router to support Cisco Unified CME or Cisco Unity Express, you will be required to install hardware components.
Voice bundles do not include all the necessary components for Cisco Unity Express. Contact the Cisco IP Communications Express partner in your area for more information about including Cisco Unity Express in your configuration.

Before You Begin

- Cisco router and all recommended hardware for Cisco Unified CME, and if required, Cisco Unity Express, is ordered and delivered, or is already onsite.

Step 1 Install the Cisco router on your network. To find installation instructions for the Cisco router, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Routers>***router you are using***>Install and Upgrade Guides**.

Step 2 Install Cisco voice services hardware.

a) To find installation instructions for any Cisco interface card, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Cisco Interfaces and Modules>***interface you are using***>Install and Upgrade Guides** or Documentation Roadmap.
b) To install and configure your Catalyst switch, see Cisco Network Assistant.
c) To find installation instructions for any Cisco EtherSwitch module, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Cisco Switches>***switch you are using***>Install and Upgrade Guides**.

Step 3 Connect to the Cisco router using a terminal or PC with terminal emulation. Attach a terminal or PC running terminal emulation to the console port of the router.

Use the following terminal settings:

- 9600 baud rate
- No parity
- 8 data bits
- 1 stop bit
- No flow control

Note Memory recommendations and maximum numbers of Cisco IP phones identified in the next step are for common Cisco Unified CME configurations only. Systems with large numbers of phones and complex configurations may not work on all platforms and can require additional memory or a higher performance platform.

Step 4 Log in to the router and use the **show version** EXEC command or the **show flash** privileged EXEC command to check the amount of memory installed in the router. Look for the following lines after issuing the **show version** command.

Example:

```
Router> show version...
Cisco 2691 (R7000) processor (revision 0.1) with 177152K/19456K bytes of memory
...
31360K bytes of ATA System Compactflash (Read/Write)
```

The first line indicates how much Dynamic RAM (DRAM) and Packet memory is installed in your router. Some platforms use a fraction of their DRAM as Packet memory. The memory requirements take this into account, so you have to add both numbers to find the amount of DRAM available on your router (from a memory requirement point of view).

The second line identifies the amount of flash memory installed in your router.

or

Look for the following line after issuing the **show flash** command. Add the number available to the number used to determine the total flash memory installed in the Cisco router.

```
Router# show flash
...
2252800 bytes available, (29679616 bytes used]
```

Step 5 Identify DRAM and flash memory requirements for the Cisco Unified CME version and Cisco router model you are using. To find Cisco Unified CME specifications, see the appropriate Cisco Unified CME Supported Firmware, Platforms, Memory, and Voice Products.

Step 6 Compare the amount of memory required to the amount of memory installed in the router. To install or upgrade the system memory in the router, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Routers>*router you are using*>Install and Upgrade Guides**.

Step 7 Use the **memory-size iomem** *i/o memory-percentage* privileged EXEC command to disable Smartinit and allocate ten percent of the total memory to Input/Output (I/O) memory.

Example:

```
Router# memory-size iomem 10
```

Install Cisco IOS Software

Note The Cisco router in a voice bundle is preloaded with the recommended Cisco IOS software release and feature set plus the necessary Cisco Unified CME phone firmware and GUI files to support Cisco Unified CME and Cisco Unity Express. If the recommended software is not installed or if you are upgrading an existing Cisco router to support Cisco Unified CME and Cisco Unity Express, you will be required to download and extract the required image and files.

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

Before You Begin

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

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

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

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

Step 3 If required, download and extract the recommended Cisco IOS IP Voice or higher image to flash memory in the router. To find software installation information, access information located at **www.cisco.com>Technical Support & Documentation>Product Support> Cisco IOS Software>*Cisco IOS Software Mainline release you are using*> Configuration Guides> Cisco IOS Configuration Fundamentals and Network Management Configuration Guide>Part 2: File Management>Locating and Maintaining System Images**.

Step 4 To reload the Cisco Unified CME router with the new software after replacing or upgrading the Cisco IOS release, use the **reload** privileged EXEC command.
Example:

```
Router# reload
System configuration has been modified. Save [yes/no]:
Y
Building configuration...
OK
Proceed with reload? Confirm.
11w2d: %Sys-5-RELOAD: Reload requested by console. Reload reason: reload command . System bootstrap,
 System Version 12.2(8r)T, RELEASE SOFTWARE (fc1)
...
Press RETURN to get started.
...
Router>
```

What to Do Next

- If you installed a new Cisco IOS software release on the Cisco router, download and extract the compatible Cisco Unified CME version. See Install and Upgrade Cisco Unified CME Software, on page 101.
- If you are installing a new stand-alone Cisco Unified CME system, see Configure VLANs on a Cisco Switch, on page 90.

Configure VLANs on a Cisco Switch

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, on a Cisco Catalyst switch or an internal Cisco NM, HWIC, or Fast Ethernet switching module, perform only *one* of the following tasks.

- Network Assistant, on page 90
- Cisco IOS Commands, on page 91
- Internal Cisco Ethernet Switching Module, on page 94

Network Assistant

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, on an external Cisco Catalyst switch and to implement Cisco Quality-of-Service (QoS) policies on your network, perform the following steps.

Before You Begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware and other optional hardware.
- The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware and GUI files are installed.

- Determine if you can use the Cisco Network Assistant to configure VLANs on the switch for your Cisco Unified CME router, see *Devices Supported* in the appropriate Release Notes for Cisco Network Assistant.

Note A PC connected to the Cisco Unified CME router over the LAN is required to download, install, and run Cisco Network Assistant.

- If you want to use Cisco Network Assistant to configure VLANs on the Cisco Catalyst switch, verify that the PC on which you want to install and run Cisco Network Assistant meets the minimum hardware and operating system requirements. See *Installing, Launching, and Connecting Network Assistant* in Getting Started with Cisco Network Assistant.
- An RJ-45-to-RJ-45 rollover cable and the appropriate adapter (both supplied with the switch) connecting the RJ-45 console port of the switch to a management station or modem is required to manage a Cisco Catalyst switch through the management console.

Step 1 Install, launch, and connect Cisco Network Assistant. For instructions, see *Installing, Launching, and Connecting Network Assistant* in Getting Started with Cisco Network Assistant.

Step 2 Use Cisco Network Assistant to perform the following tasks. See online Help for additional information and procedures.

- Enable two VLANs on the switch port.
- Configure a trunk between the Cisco Unified CME router and the switch.
- Configure Cisco IOS Quality-of-Service (QoS).

Cisco IOS Commands

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, a trunk between the Cisco Unified CME router and the switch, and Cisco IOS Quality-of-Service (QoS) on an external Cisco Catalyst switch, perform the following steps.

Before You Begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware and other optional hardware.
- The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware and GUI file are installed.
- An RJ-45-to-RJ-45 rollover cable and the appropriate adapter (both supplied with the switch) connecting the RJ-45 console port of the switch to a management station or modem is required to manage a Cisco Catalyst switch through the management console.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vlan** *vlan-number* **name** *vlan-name*
4. **vlan** *vlan-number* **name** *vlan-name*
5. **exit**
6. **wr**
7. **configure terminal**
8. **macro global apply cisco-global**
9. **interface** *slot-number* / *port-number*
10. **macro apply cisco-phone $AVID** *number* **$VVID** *number*
11. **interface** *slot-number* / *port-number*
12. **macro apply cisco-router $NVID** *number*
13. **end**
14. **wr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Switch# vlan database`	Enters VLAN configuration mode.

Step 3	**vlan** *vlan-number* **name** *vlan-name*
	
	Example:
	`Switch(vlan)# vlan 10 name data`
	`VLAN 10 modified`
	`Name: DATA`
		Specifies the number and name of the VLAN being configured.
		• *vlan-number*—Unique value that you assign to the dial-peer being configured. Range: 2 to 1004.
		• *name*—Name of the VLAN to associate to the vlan-number being configured.

Step 4	**vlan** *vlan-number* **name** *vlan-name*
	
	Example:
	`Switch(vlan)# vlan 100 name voice`
	`VLAN 100 modified`
	`Name: VOICE`
		Specifies the number and name of the VLAN being configured.

Step 5	**exit** **Example:** `Switch(vlan)# exit`	Exits this configuration mode.

	Command or Action	Purpose
Step 6	**wr** **Example:** `Switch# wr`	Writes the modifications to the configuration file.
Step 7	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 8	**macro global apply cisco-global** **Example:** `Switch (config)# macro global apply cisco-global`	Applies the Smartports global configuration macro for QoS.
Step 9	**interface** *slot-number* / *port-number* **Example:** `Switch (config)# interface fastEthernet 0/1`	Specifies interface to be configured while in the interface configuration mode. • *slot-number/port-number*—Slot and port of interface to which Cisco IP phones or PCs are connected. **Note** The slash must be entered between the slot and port numbers.
Step 10	**macro apply cisco-phone $AVID** *number* **$VVID** *number* **Example:** `Switch (config-if)# macro apply cisco-phone $AVID 10 $VVID 100`	Applies VLAN and QoS settings in Smartports macro to the port being configured. • **$AVID** *number*—Data VLAN configured in earlier step. • **$VVID** *number*—Voice VLAN configured in earlier step.
Step 11	**interface** *slot-number* / *port-number* **Example:** `Switch (config-if)# interface fastEthernet 0/24`	Specifies interface to be configured while in the interface configuration mode. • *slot-number/port-number*—Slot and port of interface to which the Cisco router is connected. **Note** The slash must be entered between the slot and port numbers.
Step 12	**macro apply cisco-router $NVID** *number* **Example:** `Switch (config-if)# macro apply cisco-router $NVID 10`	Applies the VLAN and QoS settings in Smartports macro to the port being configured. • **$NVID** *number*—Data VLAN configured in earlier step.
Step 13	**end** **Example:** `Switch(config-if)# end`	Exits to privileged EXEC configuration mode.

	Command or Action	Purpose
Step 14	**wr** **Example:** `Switch# wr`	Writes the modifications to the configuration file.

What to Do Next

See Using Cisco IOS Commands, on page 95.

Internal Cisco Ethernet Switching Module

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, on an internal Cisco Ethernet switching module, perform the following steps.

Before You Begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware and other optional hardware.
- The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware and GUI files are installed.
- The switch is in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vlan** *vlan-number* **name** *vlan-name*
4. **vlan** *vlan-number* **name** *vlan-name*
5. **exit**
6. **wr**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**vlan database** **Example:** `Switch#` **vlan database**	Enters VLAN configuration mode.

Step 3	**vlan** *vlan-number* **name** *vlan-name*
	
	Example:
	`Switch(vlan)# vlan 10 name data`
	`VLAN 10 modified Name: DATA`
		Specifies the number and name of the VLAN being configured.
		• *vlan-number*—Unique value that you assign to dial-peer being configured. Range: 2 to 1004.
		• *name*—Name of the VLAN to associate to the vlan-number being configured.

Step 4	**vlan** *vlan-number* **name** *vlan-name*
	
	Example:
	`Switch(vlan)#` **vlan 100 name voice**
	`VLAN 100 modified`
	`Name: VOICE`
		Specifies the number and name of the VLAN being configured.

Step 5	**exit** **Example:** `Switch(vlan)#` **exit**	Exits this configuration mode.
Step 6	**wr** **Example:** `Switch#` **wr**	Writes the modifications to the configuration file.

What to Do Next

See Using Cisco IOS Commands, on page 95.

Using Cisco IOS Commands

Prerequisites

- Hardware and software to establish a physical or virtual console connection to the Cisco router using a terminal or PC running terminal emulation is available and operational.
- Connect to the Cisco router using a terminal or PC with terminal emulation. Attach a terminal or PC running terminal emulation to the console port of the router.
  For connecting to the router to be configured, use the following terminal settings:
    - 9600 baud rate
    - No parity
    - 8 data bits

  - 1 stop bit
  - No flow control

Your choice of configuration method depends on whether you want to create an initial configuration for your IP telephony system or you want to perform ongoing maintenance, such as routinely making additions and changes associated with employee turnover. Table 5: Comparison of Configuration Methods for Cisco Unified CME, on page 96 compares the different methods for configuring Cisco Unified CME.

Table 5: Comparison of Configuration Methods for Cisco Unified CME

Configuration Method	Benefits	Restrictions
Cisco IOS command line interface	• Generates commands for running configuration which can be saved on Cisco router to be configured. • Use for setting up or modifying all parameters and features during initial configuration and ongoing maintenance.	Requires knowledge of Cisco IOS commands and Cisco Unified CME.
Cisco Unified CME GUI, on page 98	• Graphical user interface • Use for ongoing system maintenance • Modifies, adds, and deletes phones and extensions; configures voice-mail; IP phone URLs; secondary dial tone pattern; timeouts; transfer patterns; and the music-on-hold file. • Three configurable levels of access.	• Cannot provision voice features such as digit translation, call routing, and class of restriction. • Cannot provision data features such as DHCP, IP addressing, and VLANs. • Can only provision IP phones that are registered to Cisco Unified CME. Cannot use bulk administration to import multiple phones at the same time. Cannot manage IP phone firmware. • Requires manual upgrade of files in flash if Cisco Unified CME version is upgraded.

Voice Bundles

Voice bundles include a Cisco Integrated Services Router for secure data routing, Cisco Unified CME software and licenses to support IP telephony, Cisco IOS SP Services or Advanced IP Services software for voice gateway features, and the flexibility to add Cisco Unity Express for voice mail and auto attendant capabilities. Voice bundles are designed to meet the diverse needs of businesses worldwide. To complete the solution, add digital or analog trunk interfaces to interface to the PSTN or the host PBX, Cisco IP phones, and Cisco Catalyst data switches supporting Power-over Ethernet (PoE).

Table 6: Cisco Tools for Deploying Cisco IPC Express, on page 97 contains a list of the Cisco tools for deploying Cisco IPC Express.

Table 6: Cisco Tools for Deploying Cisco IPC Express

Tool Name	Description
Cisco Configuration Professional Express (Cisco CP Express) and Cisco Configuration Professional (Cisco CP)	Cisco CP Express is a basic router configuration tool that resides in router Flash memory. It is shipped with every device ordered with Cisco CP. Cisco CP Express allows the user to give the device a basic configuration, and allows the user to install Cisco CP for advanced configuration and monitoring capabilities. Cisco CP is the next generation advanced configuration and monitoring tool. It enables you to configure such things as router LAN and WAN interfaces, a firewall, IPSec VPN, dynamic routing, and wireless communication. Cisco CP is installed on a PC. It is available on a CD, and can also be downloaded from www.cisco.com.
Cisco Unified CME GUI, on page 98	Cisco Unified CME GUI enables the user to configure a subset of optional system and phone features.
Cisco Network Assistant	Cisco Network Assistant is a PC-based network management application optimized for networks of small and medium-sized businesses. Through a user-friendly GUI, the user can apply common services such as configuration management, inventory reports, password synchronization and Drag and Drop IOS Upgrade across Cisco SMB-Class switches, routers and access points.
Initialization Wizard for Cisco Unity Express See *Configuring the System for the First Time*, in the appropriate Cisco Unity Express GUI Administrator Guide.	Initialization Wizard in the Cisco Unity Express GUI prompts the user for required information to configure users, voice mailboxes, and other features of voice mail and auto attendant. The wizard starts automatically the first time you log in to the Cisco Unity Express GUI.

Tool Name	Description
Router and Security Device Manager (SDM)	Cisco Router and Security Device Manager (Cisco SDM) is an intuitive, Web-based device-management tool for Cisco routers. Cisco SDM simplifies router and security configuration through smart wizards, which help customers and Cisco partners quickly and easily deploy, and configure a Cisco router without requiring knowledge of the command-line interface (CLI). Supported on Cisco 830 Series to Cisco 7301 routers, Cisco SDM is shipping on Cisco 1800 Series, Cisco 2800 Series, and Cisco 3800 Series routers pre-installed by the factory.

Cisco Unified CME GUI

The Cisco Unified CME GUI provides a web-based interface to manage most system-level and phone-level features. In particular, the GUI facilitates the routine additions and changes associated with employee turnover, allowing these changes to be performed by nontechnical staff.

The GUI provides three levels of access to support the following user classes:

- System administrator—Able to configure all systemwide and phone-based features. This person is familiar with Cisco IOS software and VoIP network configuration.
- Customer administrator—Able to perform routine phone additions and changes without having access to systemwide features. This person does not have to be familiar with Cisco IOS software.
- Phone user—Able to program a small set of features on his or her own phone and search the Cisco Unified CME directory.

The Cisco Unified CME GUI uses HTTP to transfer information between the Cisco Unified CME router and the PC of an administrator or phone user. The router must be configured as an HTTP server, and an initial system administrator username and password must be defined. Additional customer administrators and phone users can be added by using Cisco IOS command line interface or by using GUI screens.

Cisco Unified CME provides support for eXtensible Markup Language (XML) cascading style sheets (files with a .css suffix) that can be used to customize the browser GUI display.

The GUI supports authentication, authorization, and accounting (AAA) authentication for system administrators through a remote server capability. If authentication through the server fails, the local router is searched.

Cisco Unified CME GUI must be installed and set up before it can be used. Instructions for using the Cisco Unified GUI are in online help for the GUI.

To use the Cisco Unified CME GUI to modify the configuration, see online help.

Prerequisites

- Cisco CME 3.2 or a later version.

- Files required for the operation of the GUI must be copied into flash memory on the router. For information about files, see Install and Upgrade Cisco Unified CME Software, on page 101.
- Cisco Unified CME GUI must be enabled. For information, see Enable the GUI, on page 525.

Restrictions

- The web browser that you use to access the GUI must be Microsoft Internet Explorer 5.5 or a later version. No other type of browser can be used to access the GUI.
- Cannot provision voice features such as digit translation, call routing, and class of restriction.
- Cannot provision data features such as DHCP, IP addressing, and VLANs.
- Can only provision IP phones that are registered to Cisco Unified CME. Cannot use bulk administration to import multiple phones at the same time. Cannot manage IP phone firmware.
- Requires manual upgrade of files in flash memory of router if Cisco Unified CME is upgraded to later version.
- Other minor limitations, such as:
    - If you use an XML configuration file to create a customer administrator login, the size of that XML file must be 4000 bytes or smaller.
    - The password of the system administrator cannot be changed through the GUI. Only the password of a customer administrator or a phone user can be changed through the GUI.
    - If more than 100 phones are configured, choosing to display all phones will result in a long delay before results are shown.

CHAPTER 4

Install and Upgrade Cisco Unified CME Software

Prerequisites for Installing Cisco Unified CME Software

Hardware

- Your IP network is operational and you can access Cisco web.
- You have a valid Cisco.com account.
- You have access to a TFTP server for downloading files.
- Cisco router and all recommended services hardware for Cisco Unified CME is installed. For installation information, see Install Cisco Voice Services Hardware, on page 87.

Cisco IOS Software

- Recommended Cisco IOS IP Voice or higher image is downloaded to flash memory in the router. To determine which Cisco IOS software release supports the recommended Cisco Unified CME version, see Cisco Unified CME and Cisco IOS Software Compatibility Matrix. For installation information, see Install Cisco IOS Software, on page 89.

Cisco Unified CME Software

This section contains a list of the types of files that must be downloaded and installed in the router flash memory to use with Cisco Unified CME. The files listed in this section are included in zipped or tar archives that are downloaded from the Cisco Unified CME software download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Basic Files

A tar archive contains the basic files you need for Cisco Unified CME. Be sure to download the correct version for the Cisco IOS software release that is running on your router. The basic tar archive generally also contains the phone firmware files that you require, although you may occasionally need to download individual phone firmware files. For information about installing Cisco Unified CME, see Install Cisco Unified CME Software, on page 105.

GUI Files

A tar archive contains the files that you need to use the Cisco Unified CME graphical user interface (GUI), which provides a mouse-driven interface for provisioning phones after basic installation is complete. For installation information, see Install Cisco Unified CME Software, on page 105.

Note Cisco Unified CME GUI files are version-specific; GUI files for one version of Cisco Unified CME are not compatible with any other version of Cisco Unified CME. When downgrading or upgrading Cisco Unified CME, the GUI files for the old version must be overwritten with GUI files that match the Cisco Unified CME version that is being installed.

Phone Firmware Files

Phone firmware files provide code to enable phone displays and operations. These files are specialized for each phone type and protocol, SIP or SCCP, and are periodically revised. You must be sure to have the appropriate phone firmware files for the types of phones, protocol being used, and Cisco Unified CME version at your site.

New IP phones are shipped from Cisco with a default manufacturing SCCP image. When a IP phone downloads its configuration profile, the phone compares the phone firmware mentioned in the configuration profile with the firmware already installed on the phone. If the firmware version differs from the one that is currently loaded on the phone, the phone contacts the TFTP server to upgrade to the new phone firmware and downloads the new firmware before registering with Cisco Unified CME.

Generally, phone firmware files are included in the Cisco Unified CME software archive that you download. They can also be posted on the software download website as individual files or archives.

Early versions of Cisco phone firmware for SCCP and SIP IP phones had filenames as follows:

- SCCP firmware—P003xxyy.bin
- SIP firmware—P0S3xxyy.bin

In both bases, x represents the major version, and y represented the minor version. The third character represents the protocol, “0” for SCCP or “S” for SIP.

In later versions, the following conventions are used:

- SCCP firmware—P003xxyyzzww, where x represents the major version, y represents the major subversion, z represents the maintenance version, and w represents the maintenance subversion.

- SIP firmware—P0S3-xx-y-zz, where x represents the major version, y represents the minor version, and z represents the subversions.
- The third character in a filename—Represents the protocol, “0” for SCCP or “S” for SIP.

There are exceptions to the general guidelines. For Cisco ATA, the filename begins with AT. For Cisco Unified IP Phone 7002, 7905, and 7912, the filename can begin with CP.

Signed and unsigned versions of phone firmware are available for certain phone types. Signed binary files support image authentication, which increases system security. We recommend signed versions if your version of Cisco Unified CME supports them. Signed binary files have .sbn file extensions, and unsigned files have .bin file extensions.

For Java-based IP phones, such as the Cisco Unified IP Phone 7911, 7941, 7941GE, 7961, 7961GE, 7970, and 7971, the firmware consists of multiple files including JAR and tone files. All of the firmware files for each phone type must be downloaded the TFTP server before they can be downloaded to the phone.

The following example shows a list of phone firmware files that are installed in flash memory for the Cisco Unified IP Phone 7911:

```
tftp-server flash:SCCP11.7-2-1-0S.loads
tftp-server flash:term06.default.loads
tftp-server flash:term11.default.loads
tftp-server flash:cvm11.7-2-0-66.sbn
tftp-server flash:jar11.7-2-0-66.sbn
tftp-server flash:dsp11.1-0-0-73.sbn
tftp-server flash:apps11.1-0-0-72.sbn
tftp-server flash:cnu11.3-0-0-81.sbn
```

However, you only specify the filename for the image file when configuring Cisco Unified CME. For Java-based IP phones, the following naming conventions are used for image files:

- SCCP firmware—TERMnn.xx-y-z-ww or SCCPnn.xx-y-zz-ww, where n represents the phone type, x represents the major version, y represents the major subversion, z represents the maintenance version, and w represents the maintenance subversion.

The following example shows how to configure Cisco Unified CME so that the Cisco Unified IP Phone 7911 can download the appropriate SCCP firmware from flash memory:

```
Router(config)# telephony-service
Router(config-telephony)#load 7911 SCCP11.7-2-1-0S
```

Table 7: Firmware-Naming Conventions, on page 103 contains firmware-naming convention examples, in alphabetical order:

Table 7: Firmware-Naming Conventions

SCCP Phones		SIP Phones	
Image	**Version**	**Image**	**Version**
P00303030300	3.3(3)	P0S3-04-4-00	4.4
P00305000200	5.0(2)	P0S3-05-2-00	5.2
P00306000100	6.0(1)	P0S3-06-0-00	6.0

SCCP Phones		SIP Phones	
SCCP41.8-0-4ES4-0-1S	8.0(4)	SIP70.8-0-3S	8.0(3)
TERM41.7-0-3-0S	7.0(3)	—	—

The phone firmware filenames for each phone type and Cisco Unified CME version are listed in the appropriate document available at Cisco CME Supported Firmware, Platforms, Memory, and Voice Products.

For information about installing firmware files, see Install Cisco Unified CME Software, on page 105.

For information about configuring Cisco Unified CME for upgrading between versions or converting between SCCP and SIP, see Install and Upgrade Cisco Unified CME Software, on page 101.

XML Template

The file called xml.template can be copied and modified to allow or restrict specific GUI functions to customer administrators, a class of administrative users with limited capabilities in a Cisco Unified CME system. This file is included in both tar archives (cme-basic-... and cme-gui-...). To install the file, see Install Cisco Unified CME Software, on page 105.

Music-on-Hold (MOH) File

An audio file named music-on-hold.au provides music for external callers on hold when a live feed is not used. This file is included in the tar archive with basic files (cme-basic-...). To install the file, see Install Cisco Unified CME Software, on page 105.

Script Files

Archives containing Tcl script files are listed individually on the Cisco Unified CME software download website. For example, the file named app-h450-transfer.2.0.0.9.zip.tar contains a script that adds H.450 transfer and forwarding support for analog FXS ports.

The Cisco Unified CME Basic Automatic Call Distribution and Auto Attendant Service (B-ACD) requires a number of script files and audio files, which are contained in a tar archive with the name cme-b-acd-.... For a list of files in the archive and for more information about the files, see Cisco CME B-ACD and TCL Call-Handling Applications.

For information about installing Tcl script file or an archive, see Install Cisco Unified CME Software, on page 105.

Bundled TSP Archive

An archive is available at the Cisco Unified CME software download website that contains several Telephony Application Programming Interface (TAPI) Telephony Service Provider (TSP) files. These files are needed to set up individual PCs for Cisco Unified IP phone users who wish to make use of Cisco Unified CME-TAPI integration with TAPI-capable PC software. To install the files from the archive, see the installation instructions in TAPI Developer Guide for Cisco CME/SRST.

File Naming Conventions

Most of the files available at the Cisco Unified CME software download website are archives that must be uncompressed before individual files can be copied to the router. In general, the following naming conventions apply to files on the Cisco Unified CME software download website:

Table 8: File Naming Conventions

`cme-basic-...`	Basic Cisco Unified CME files, including phone firmware files for a particular Cisco Unified CME version or versions.
`cme-gui-...`	Files required for the Cisco Unified CME GUI.
`cmterm..., P00..., 7970..`	Phone firmware files. **Note** Not all firmware files to be downloaded to a phone are specified in the **load** command. For a list of file names to be installed in flash memory, and which file names are to be specified by using the **load** command, see Cisco Unified CME Supported Firmware, Platforms, Memory, and Voice Products.
`cme-b-acd...`	Files required for Cisco Unified CME B-ACD service.

Install and Upgrade Cisco Unified CME Software

Note Customers who purchase a router bundle enabled with Cisco Unified CME will have the necessary Cisco Unified CME files installed at time of manufacture.

Install Cisco Unified CME Software

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key.

Step 2 Select the file to download.

Step 3 Download zip file to tftp server.

Step 4 Use the zip program to extract the file to be installed, then:

a) If the file is an individual file, use the **copy** command to copy the files to router flash:
`Router#` **copy tftp://x.x.x.x/P00307020300.sbn flash:**

b) If the file is a tar file, use the **archive tar**command to extract the files to flash memory.
`Router#` **archive tar /xtract** *source-url***flash:***/file-url*

Step 5 Verify the installation. Use the **show flash:** command to list the files installed in in flash memory.

```
Router# show flash:

 31      128996 Sep 19 2005 12:19:02 -07:00 P00307020300.bin
 32         461 Sep 19 2005 12:19:02 -07:00 P00307020300.loads
 33      681290 Sep 19 2005 12:19:04 -07:00 P00307020300.sb2
 34      129400 Sep 19 2005 12:19:04 -07:00 P00307020300.sbn
```

Step 6 Use the **archive tar /create** command to create a backup tar file of all the files stored in flash. You can create a tar file that includes all files in a directory or a list of up to four files from a directory.
For example, the following command creates a tar file of the three files listed:

archive tar /create flash:abctestlist.tar flash:orig1 sample1.txt sample2.txt sample3.txt

The following command creates a tar file of all the files in the directory:

archive tar /create flash:abctest1.tar flash:orig1

The following command creates a tar file to backup the flash files to a USB card, on supported platforms:

archive tar /create usbflash1:abctest1.tar flash:orig1

What to Do Next

- If you installed Cisco Unified CME software and Cisco Unified CME is *not* configured on your router, see Network Parameters, on page 121.
- If Cisco Unified IP phones presently connected to Cisco Unified CME are using the SCCP protocol to receive and place calls and the firmware version must be upgraded to a recommended version, or if the phones to be connected to Cisco Unified CME are brand new, out-of-the-box, the phone firmware preloaded at the factory must be upgraded to the recommended version before your phones can complete registration, see Upgrade or Downgrade SCCP Phone Firmware, on page 107.
- If Cisco Unified IP phones presently connected to Cisco Unified CME are using the SIP protocol to receive and place calls and the firmware version must be upgraded to a recommended version, see Upgrade or Downgrade SIP Phone Firmware, on page 108.
- If Cisco Unified IP phones presently connected to Cisco Unified CME are using the SCCP protocol to receive and place calls and you now want some or all of these phones to use the SIP protocol, the phone firmware for each phone type must be upgraded from SCCP to the recommended SIP version before the phones can register. See Phone Firmware Conversion from SCCP to SIP, on page 112.
- If Cisco Unified IP phones to be connected to Cisco Unified CME are using the SIP protocol and are brand new, out-of-the-box, the phone firmware preloaded at the factory must be upgraded to the recommended SIP version before your SIP phones can complete registration. See Phone Firmware Conversion from SCCP to SIP, on page 112.
- If Cisco Unified IP phones presently connected to Cisco Unified CME are using the SIP protocol to receive and place calls and you now want some or all of these phones to use the SCCP protocol, the phone firmware for each phone type must be upgraded from SIP to the recommended SCCP version before the phones can register. See Phone Firmware Conversion from SIP to SCCP, on page 115.

Upgrade or Downgrade SCCP Phone Firmware

Note For certain IP phones, such as the Cisco Unified IP Phone 7911, 7941, 7961, 7970, and 7971, the firmware consists of multiple files including JAR and tone files. All of the firmware files must be downloaded to the TFTP server before they can be downloaded to the phone. For a list of files in each firmware version, see the appropriate Cisco Unified CME Supported Firmware, Platforms, Memory, and Voice Products.

Before You Begin

- Phone firmware for Cisco Unified IP phones to be connected to Cisco Unified CME, including all versions required during an upgrade or downgrade sequence, must be loaded in the flash memory of the TFTP server from which the phones download their configuration profiles. For information about installing firmware files in flash memory, see Install Cisco Unified CME Software, on page 105.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tftp-server** *device***:***firmware-file*
4. **telephony-service**
5. **load** *phone-type firmware-file*
6. **create cnf-files**
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	**tftp-server** *device***:***firmware-file*
	
	Example:
	`Router(config)# tftp-server flash:P00307020300.loads`
	`Router(config)# tftp-server flash:P00307020300.sb2`
	`Router(config)# tftp-server flash:P00307020300.sbn`
	`Router(config)# tftp-server flash:P00307020300.bin`
		(Optional) Creates TFTP bindings to permit IP phones served by the Cisco Unified CME router to access the specified file.
		• A separate **tftp-server** command is required for each phone type.
		• Required for Cisco Unified CME 7.0/4.3 and earlier versions.
		• Cisco Unified CME 7.0(1) and later versions: Required only if the location for cnf files is *not* flash or slot 0. Use the complete

	Command or Action	Purpose
		filename, including the file suffix, for phone firmware versions later than version 8-2-2 for all phone types.
Step 4	**telephony-service** **Example:** `Router(config)# telephony service`	Enters telephony-service configuration mode.
Step 5	**load** *phone-type firmware-file* **Example:** `Router(config-telephony)# load 7960-7940 P00307020300`	Associates a phone type with a phone firmware file. • A separate **load** command is required for each IP phone type. • *firmware-file*—Filenames are case-sensitive. • In Cisco Unified CME 7.0/4.3 and earlier versions, do not use the file suffix (.bin, .sbin, .loads) for any phone type except the Cisco ATA and Cisco Unified IP Phone 7905 and 7912. • In Cisco Unified CME 7.0(1) and later versions, you must use the complete filename, including the file suffix, for phone firmware versions later than version 8-2-2 for all phone types.
Step 6	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds XML configuration files required for SCCP phones.
Step 7	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

What to Do Next

- If the Cisco Unified IP phone to be upgraded is not configured in Cisco Unified CME, see Configure Phones for a PBX System, on page 253.
- If the Cisco Unified IP phone is already configured in Cisco Unified CME and can make and receive calls, you are ready to reboot the Cisco Unified IP phones to download the phone firmware to the phone. See Reset and Restart Cisco Unified IP Phones, on page 397.

Upgrade or Downgrade SIP Phone Firmware

The upgrade and downgrade sequences for SIP phones differ per phone type as follows:

- Upgrading/downgrading the phone firmware for Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7912G, and Cisco ATA Analog Telephone Adapter is straightforward; modify the **load** command to upgrade directly to the target load.

- The phone firmware version upgrade sequence for Cisco Unified IP Phone 7940Gs and 7960Gs is from version [234].x to 4.4, to 5.3, to 6.x, to 7.x. You cannot go directly from version [234].x to version 7.x.
- To downgrade phone firmware for Cisco Unified IP Phone 7940Gs and 7960Gs, first upgrade to version 7.x, then modify the **load** command to downgrade directly to the target phone firmware.

Restriction

- Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7912G, and Cisco ATA—Signed load starts from SIP v1.1. After you upgrade the firmware to a signed load, you cannot downgrade the firmware to an unsigned load.
- Cisco Unified IP Phone 7940G and Cisco Unified IP Phone 7960G—Signed load starts from SIP v5.x. Once you upgrade the firmware to a signed load, you cannot downgrade the firmware to an unsigned load.
- The procedures for upgrading phone firmware files for SIP phones is the same for all Cisco Unified IP phones. For other limits on firmware upgrade between versions, see Cisco 7940 and 7960 IP Phones Firmware Upgrade Matrix.

Before You Begin

Phone firmware for Cisco Unified IP phones to be connected to Cisco Unified CME, including all versions required during an upgrade or downgrade sequence, must be loaded in the flash memory of the TFTP server from which the phones will download their configuration profiles. For information about installing firmware files in flash memory, see Install Cisco Unified CME Software, on page 105.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode cme**
5. **load** *phone-type firmware-file*
6. **upgrade**
7. Repeat Step 5 and Step 6.
8. **file text**
9. **create profile**
10. **exit**
11. **voice register pool** *pool-tag*
12. **reset**
13. **exit**
14. **voice register global**
15. **no upgrade**
16. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**mode cme** **Example:** `Router(config-register-global)# mode cme`	Enables mode for provisioning SIP phones in Cisco Unified CME.
Step 5	**load** *phone-type firmware-file* **Example:** `Router(config-register-global)# load 7960-7940 P0S3-06-0-00`	Associates a phone type with a phone firmware file. • A separate **load** command is required for each IP phone type. • *firmware-file*—Filename to be associated with the specified Cisco Unified IP phone type. • Do not use the .sbin or .loads file extension except for Cisco ATA and Cisco Unified IP Phone 7905 and 7912
Step 6	**upgrade** **Example:** `Router(config-register-global)# upgrade`	Generates a file with the universal application loader image for upgrading phone firmware and performs the TFTP server alias binding.

Step 7	Repeat Step 5 and Step 6.
	
	Example:
	`Router(config-register-global)# load 7960-7940 P0S3-07-4-00`
	`Router(config-register-global)# upgrade`
		(Optional) Repeat for each version required in multistep upgrade sequences only.

Step 8	**file text** **Example:** `Router(config-register-global)# file text`	(Optional) Generates ASCII text files for Cisco Unified IP Phone 7905s and 7905Gs, Cisco Unified IP Phone 7912s and 7912Gs, Cisco ATA-186, or Cisco ATA-188. • Default—System generates binary files to save disk space.

	Command or Action	Purpose
Step 9	**create profile** **Example:** `Router(config-register-global;)# create profile`	Generates provisioning files required for SIP phones and writes the file to the location specified with the **tftp-path** command.
Step 10	**exit** **Example:** `Router(config-register-global)# exit`	Exits from the current command mode to the next highest mode in the configuration mode hierarchy.
Step 11	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 1`	Enters voice register pool configuration mode to set phone-specific parameters for SIP phones. • *pool-tag*—Unique sequence number of the SIP phone to be configured. Range is 1 to 100 or the upper limit as defined by **max-pool** command.
Step 12	**reset** **Example:** `Router(config-register-pool)# reset`	Performs a complete reboot of the single SIP phone specified with the **voice register pool** command and contacts the DHCP server and the TFTP server for updated information.
Step 13	**exit** **Example:** `Router(config-register-pool)# exit`	Exits from the current command mode to the next highest mode in the configuration mode hierarchy.
Step 14	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 15	**no upgrade** **Example:** `Router(config-register-global)# no upgrade`	Return to the default for the **upgrade** command.
Step 16	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

The following example shows the configuration steps for upgrading firmware for a Cisco Unified IP Phone 7960G or Cisco Unified IP Phone 7940G from SIP 5.3 to SIP 6.0, then from SIP 6.0 to SIP 7.4:

```
Router(config)# voice register global
Router(config-register-global)# mode cme
Router(config-register-global)# load 7960 P0S3-06-0-00
Router(config-register-global)# upgrade
Router(config-register-global)# load 7960 P0S3-07-4-00
Router(config-register-global)# create profile
```

The following example shows the configuration steps for downgrading firmware for a Cisco Unified IP Phone 7960/40 from SIP 7.4 to SIP 6.0:

```
Router(config)# voice register global
Router(config-register-global)# mode cme
Router(config-register-global)# load 7960 P0S3-06-0-00
Router(config-register-global)# upgrade
Router(config-register-global)# create profile
```

What to Do Next

- If the Cisco Unified IP phone to be upgraded is not configured in Cisco Unified CME, see Configure Phones for a PBX System, on page 253.
- If the Cisco Unified IP phone is already configured in Cisco Unified CME and can make and receive calls, you are ready to reboot the Cisco Unified IP phones to download the phone firmware to the phone. See Reset and Restart Cisco Unified IP Phones, on page 397.

Phone Firmware Conversion from SCCP to SIP

If Cisco Unified IP phones presently connected to Cisco Unified CME are using the SCCP protocol to receive and place calls and you now want some or all of these phones to use the SIP protocol, the phone firmware for each phone type must be upgraded from SCCP to the recommended SIP version before the phones can register. If Cisco Unified IP phones to be connected to Cisco Unified CME are brand new, out-of-the-box, the SCCP phone firmware preloaded at the factory must be upgraded to the recommended SIP version before your SIP phones can complete registration.

Note If codec values for the dial peers of a connection do not match, the call fails. The default codec for the POTS dial peer for an SCCP phone is G.711 and the default codec for a VoIP dial peer for a SIP phone is G.729. If neither the SCCP phone nor the SIP phone in Cisco Unified CME has been specifically configured to change the codec, calls between the two IP phones on the same router will produce a busy signal caused by the mismatched default codecs. To avoid codec mismatch, specify the codec for IP phones in Cisco Unified CME. For configuration information, see Configure Individual IP Phones for Key System on SCCP Phone, on page 293.

Before You Begin

- Phone firmware for Cisco Unified IP phones to be connected to Cisco Unified CME, including all versions required during an upgrade or downgrade sequence, must be loaded in the flash memory of the TFTP server from which the phones download their configuration profiles. For information about installing firmware files in flash memory, see Install Cisco Unified CME Software, on page 105.

- Cisco Unified IP Phone 7940Gs and Cisco Unified IP Phone 7960Gs—If these IP phones are already configured in Cisco Unified CME to use the SCCP protocol, the SCCP phone firmware on the phone must be version 5.x. If required, upgrade the SCCP phone firmware to 5.x before upgrading to SIP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ephone** *ephone-tag*
4. **exit**
5. **no ephone-dn** *dn-tag*
6. **exit**
7. **voice register global**
8. **mode cme**
9. **load** *phone-type firmware-file*
10. **upgrade**
11. Repeat Step 9 and Step 10.
12. **create profile**
13. **file text**
14. **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	**no ephone** *ephone-tag* **Example:** `Router (config)# no ephone 23`	(Optional) Disables the ephone and removes the ephone configuration. • Required only if the Cisco Unified IP phone to be configured is already connected to Cisco Unified CME and is using SCCP protocol. • *ephone-tag*—Particular IP phone to which this configuration change will apply.
Step 4	**exit** **Example:** `Router(config-ephone)# exit`	(Optional) Exits from the current command mode to the next highest mode in the configuration mode hierarchy. • Required only if you performed the previous step.

	Command or Action	Purpose
Step 5	**no ephone-dn** *dn-tag*	(Optional) Disables the ephone-dn and removes the ephone-dn configuration. • Required only if this directory number is not now nor will be associated to any SCCP phone line, intercom line, paging line, voice-mail port, or message-waiting indicator (MWI) connected to Cisco Unified CME. • *dn-tag*—Particular configuration to which this change will apply.
Step 6	**exit** **Example:** `Router(config-ephone-dn)# exit`	(Optional) Exits from the current command mode to the next highest mode in the configuration mode hierarchy. • Required only if you performed the previous step.
Step 7	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 8	**mode cme** **Example:** `Router(config-register-global)# mode cme`	Enables mode for provisioning SIP phones in Cisco Unified CME.
Step 9	**load** *phone-type firmware-file* **Example:** `Router(config-register-global)# load 7960-7940 P0S3-06-3-00`	Associates a phone type with a phone firmware file. • A separate **load** command is required for each IP phone type.
Step 10	**upgrade** **Example:** `Router(config-register-global)# upgrade`	Generates a file with the universal application loader image for upgrading phone firmware and performs the TFTP server alias binding.

Step 11	Repeat Step 9 and Step 10.
	Example:
	`Router(config-register-global)# load 7960-7940 P0S3-07-4-00`
	`Router(config-register-global)# upgrade`
		(Optional) Repeat for each version required in multistep upgrade sequences only.

Step 12	**create profile** **Example:** `Router(config-register-global)# create profile`	Generates provisioning files required for SIP phones and writes the file to the location specified with the **tftp-path** command.

	Command or Action	Purpose
Step 13	**file text** **Example:** `Router(config-register-global)# file text`	(Optional) Generates ASCII text files for Cisco Unified IP Phones 7905 and 7905G, Cisco Unified IP Phone 7912 and Cisco Unified IP Phone 7912G, Cisco ATA-186, or Cisco ATA-188. • Default—System generates binary files to save disk space.
Step 14	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

The following example shows the configuration steps for converting firmware on an Cisco Unified IP phone already connected in Cisco Unified CME and using the SCCP protocol, from SCCP 5.x to SIP 7.4:

```
Router(config)# telephony-service
Router(config-telephony)# no create cnf
CNF files deleted
Router(config-telephony)# voice register global
Router(config-register-global)# mode cme
Router(config-register-global)# load 7960 P0S3-07-4-00
Router(config-register-global)# upgrade
Router(config-register-global)# create profile
```

What to Do Next

After you configure the **upgrade** command, refer to the following statements to determine which task to perform next.

- If the Cisco Unified IP phone to be upgraded is already connected in Cisco Unified CME and you removed the SCCP configuration file for the phone but have not configured this phone for SIP in Cisco Unified CME, see Configure Phones for a PBX System, on page 253.
- If the Cisco Unified IP phones to be upgraded are already configured in Cisco Unified CME, see Reset and Restart Cisco Unified IP Phones, on page 397.

Phone Firmware Conversion from SIP to SCCP

If Cisco Unified IP phones presently connected to Cisco Unified CME are using the SIP protocol to receive and place calls and you now want some or all of these phones to use the SCCP protocol, the phone firmware for each phone type must be upgraded from SIP to SCCP before the phones can register.

Note If codec values for the dial peers of a connection do not match, the call fails. The default codec for the POTS dial peer for an SCCP phone is G.711 and the default codec for a VoIP dial peer for a SIP phone is G.729. If neither the SCCP phone nor the SIP phone in Cisco Unified CME has been specifically configured to change the codec, calls between the two IP phones on the same router will produce a busy signal caused by the mismatched default codecs. To avoid codec mismatch, specify the codec for SIP and SCCP phones in Cisco Unified CME. For more information, see Configure Phones for a PBX System, on page 253.

Before You Begin

- Phone firmware for Cisco Unified IP phones to be connected to Cisco Unified CME, including all versions required during an upgrade or downgrade sequence, must be loaded in the flash memory of the TFTP server from which the phones will download their configuration profiles. For information about installing firmware files in flash memory, see Install Cisco Unified CME Software, on page 105.
- Cisco Unified IP Phone 7940Gs and Cisco Unified IP Phone 7960Gs—If these IP phones are already configured in Cisco Unified CME to use the SIP protocol, the SIP phone firmware must be version 7.x. See Upgrade or Downgrade SIP Phone Firmware, on page 108.

Remove SIP Configuration Profile

To remove the SIP configuration profile before downloading the SCCP phone firmware to convert a phone from SIP to SCCP, perform the steps in this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no voice register pool** *pool-tag*
4. **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.

	Command or Action	Purpose
Step 3	**no voice register pool** *pool-tag* **Example:** `Router(config)# no voice register pool 1`	Disables voice register pool and removes the voice pool configuration. • *pool-tag*—Unique sequence number for a particular SIP phone to which this configuration applies.
Step 4	**end** **Example:** `Router(config-register-pool)# end`	Exits from the current command mode to the next highest mode in the configuration mode hierarchy.

Generate SCCP XML Configuration File to Upgrade from SIP to SCCP

To create an ephone entry and generate a new SCCP XML configuration file for upgrading a particular Cisco Unified IP phone in Cisco Unified CME from SIP to SCCP, perform the steps in this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **exit**
5. **tftp-server** *device***:***firmware-file*
6. **telephony-service**
7. **load** *phone-type firmware-file*
8. **create cnf-files**
9. **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.

	Command or Action	Purpose
Step 3	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone dn 1`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns in Cisco Unified CME is version and platform specific. Type **?** to display range.
Step 4	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits from the current command mode to the next highest mode in the configuration mode hierarchy.

Step 5	**tftp-server** *device***:***firmware-file*
	
	Example:
	`Router(config)# tftp-server flash:P00307020300.loads`
	`Router(config)# tftp-server flash:P00307020300.sb2`
	`Router(config)# tftp-server flash:P00307020300.sbn`
	`Router(config)# tftp-server flash:P00307020300.bin`
		(Optional) Creates TFTP bindings to permit IP phones served by the Cisco Unified CME router to access the specified file.
		• A separate **tftp-server** command is required for each phone type.
		• Required for Cisco Unified CME 7.0/4.3 and earlier versions.
		• Cisco Unified CME 7.0(1) and later versions: Required only if the location for cnf files is *not* flash or slot 0. Use the complete filename, including the file suffix, for phone firmware versions later than version 8-2-2 for all phone types.

Step 6	**telephony-service** **Example:** `Router(config)# telephony service`	Enters telephony-service configuration mode.
Step 7	**load** *phone-type firmware-file* **Example:** `Router(config-telephony)# load 7960-7940 P00307020300`	Associates a phone type with a phone firmware file. • A separate **load** command is required for each IP phone type. • *firmware-file*—Filename is case-sensitive. • Cisco Unified CME 7.0/4.3 and earlier versions: Do not use the .sbin or .loads file extension except for the Cisco ATA and Cisco Unified IP Phone 7905 and 7912. • Cisco Unified CME 7.0(1) and later versions: Use the complete filename, including the file suffix, for phone firmware versions later than version 8-2-2 for all phone types.
Step 8	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds XML configuration files required for SCCP phones.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

Example

The following example shows the configuration steps for upgrading firmware for a Cisco Unified IP Phone 7960G from SIP to SCCP. First the SIP firmware is upgraded to SIP 6.3 and from SIP 6.3 to SIP 7.4; then, the phone firmware is upgraded from SIP 7.4 to SCCP 7.2(3). The SIP configuration profile is deleted and a new ephone configuration profile is created for the Cisco Unified IP phone.

```
Router(config)# v oice register global
Router(config-register-global)# mode cme
Router(config-register-global)# load 7960 P0S3-06-0-00
Router(config-register-global)# upgrade
Router(config-register-global)# load 7960 P0S3-07-4-00
Router(config-register-global)# exit
Router(config)# no voice register pool 1
Router(config-register-pool)# exit
Router(config)# v oice register global
Router(config-register-global)# no upgrade
Router(config-register-global)# exit
Router(config)# ephone-dn 1
Router(config-ephone-dn)# exit
Router(config)# tftp-server flash:P00307020300.loads
Router(config)# tftp-server flash:P00307020300.sb2
Router(config)# tftp-server flash:P00307020300.sbn
Router(config)# tftp-server flash:P00307020300.bin
Router(config)# telephony service
Router(config-telephony)# load 7960-7940 P00307000100
Router(config-telephony)# create cnf-files
```

What to Do Next

After you configure the **upgrade** command:

- If the Cisco Unified IP phone to be upgraded is already connected in Cisco Unified CME and you removed the SIP configuration file for the phone and have not configured the SCCP phone in Cisco Unified CME, see Configure Phones for a PBX System, on page 253.
- If the Cisco Unified IP phones to be upgraded are already configured in Cisco Unified CME, see Reset and Restart Cisco Unified IP Phones, on page 397.

Verify SCCP Phone Firmware Version

Step 1 **show flash:**

Use this command to learn the filenames associated with that phone firmware

Router# **show flash:**

```
31      128996 Sep 19 2005 12:19:02 -07:00 P00307020300.bin
32         461 Sep 19 2005 12:19:02 -07:00 P00307020300.loads
33      681290 Sep 19 2005 12:19:04 -07:00 P00307020300.sb2
34      129400 Sep 19 2005 12:19:04 -07:00 P00307020300.sbn
```

Step 2 **show ephone phone-load**

Use this command to verify which phone firmware is installed on a particular ephone. The DeviceName includes the MAC address for the IP phone.

Router# **show ephone phone-load**

```
DeviceName        CurrentPhoneload       PreviousPhoneload      LastReset
=====================================================================
SEP000A8A2C8C6E   7.3(3.02)                                     Initialized
```

Troubleshooting Tips for Cisco Phone Firmware

Use the **debug tftp event** command to troubleshoot an attempt to upgrade or convert Cisco phone firmware files for SIP phones.

CHAPTER 5

Network Parameters

Prerequisites for Defining Network Parameters

- IP routing must be enabled.
- VoIP networking must be operational. For quality and security purposes, we recommend you have separate virtual LANs (VLANs) for data and voice. The IP network assigned to each VLAN should be large enough to support addresses for all nodes on that VLAN. Cisco Unified CME phones receive their IP addresses from the voice network, whereas all other nodes such as PCs, servers, and printers receive their IP addresses from the data network. For configuration information, see Configure VLANs on a Cisco Switch, on page 90.
- If applicable, PSTN lines are configured and operational.
- If applicable, the WAN links are configured and operational.
- Trivial File Transfer Protocol (TFTP) must be enabled on the router to allow IP phones to download phone firmware files.
- To support IP phones that are running SIP to be directly connected to the Cisco Unified CME router, Cisco Unified CME 3.4 or later must be installed on the router.
- To provide voice-mail support for phones connected to the Cisco Unified CME router, install and configure voice mail on your network.

Restrictions for Defining Network Parameters

In Cisco Unified CME 4.0 and later versions, Layer-3-to-Layer-2 VLAN Class of Service (CoS) priority marking is not automatically processed. Cisco Unified CME 4.0 and later versions will continue to mark Layer 3, but Layer 2 marking is now only handled in the Cisco IOS software. Any Quality of Service (QoS) design that requires Layer 2 marking will have to be explicitly configured, either on a Catalyst switch that supports this capability or on the Cisco Unified CME router under the Ethernet interface configuration. For configuration information, see Enterprise QoS Solution Reference Network Design Guide.

Information About Defining Network Parameters

DHCP Service

When a Cisco Unified IP phone is connected to the Cisco Unified CME system, it automatically queries for a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server responds by assigning an IP address to the Cisco Unified IP phone and providing the IP address of the TFTP server through DHCP option 150. Then the phone registers with the Cisco Unified CME server and attempts to get configuration and phone firmware files from the TFTP server.

For configuration information, perform only *one* of the following procedures to set up DHCP service for your IP phones:

- If your Cisco Unified CME router is the DHCP server and you can use a single shared address pool for all your DHCP clients, see Configure Single DHCP IP Address Pool, on page 127.
- If your Cisco Unified CME router is the DHCP server and you need separate pools for non-IP-phone DHCP clients, see Configure Separate DHCP IP Address Pool for Each DHCP Client, on page 129.
- If the Cisco Unified CME router is not the DHCP server and you want to relay DHCP requests from IP phones to a DHCP server on a different router, see Configure DHCP Relay, on page 131.

Network Time Protocol for the Cisco Unified CME Router

Network Time Protocol (NTP) allows you to synchronize your Cisco Unified CME router to a single clock on the network, known as the clock master. NTP is disabled on all interfaces by default, but it is essential for Cisco Unified CME so you must ensure that it is enabled. For information about configuring NTP for the Cisco Unified CME router, see Enable Network Time Protocol, on page 133.

Olson Timezones

Before Cisco Unified CME 9.0, some Cisco Unified SCCP IP phones and Cisco Unified SIP IP phones displayed exactly the same time as that of the Cisco Unified CME. For these phones, the correct time was displayed whenever the Cisco Unified CME time was set correctly. The **clock timezone**, **clock summer-time**, and **clock set** commands were the only commands used to set the Cisco Unified CME time correctly.

Other phones used only the **time-zone** command in telephony-service configuration mode and the **timezone** command in voice register global configuration mode to specify which time zone they were in so that the correct local time was displayed on Cisco Unified SCCP IP phones and Cisco Unified SIP IP phones, respectively. The phones calculated and displayed the time based on the Greenwich Mean Time (GMT) provided by the Cisco Unified CME or the Network Time Protocol server. The problem with this method is that every time a new country or new time zone was available or an old time zone was changed, the Cisco Unified CME **time-zone** and **timezone** commands and the phone loads had to be updated.

In Cisco Unified CME 9.0 and later versions, the Olson Timezone feature eliminates the need to update time zone commands or phone loads to accommodate a new country with a new time zone or an existing country whose city or state wants to change their time zone. Oracle's Olson Timezone updater tool, tzupdater.jar, only needs to be current for you to set the correct time using the **olsontimezone** command in either telephony-service or voice register global configuration mode.

For Cisco Unified 3911 and 3951 SIP IP phones and Cisco Unified 6921, 6941, 6945, and 6961 SCCP and SIP IP phones, the correct Olson Timezone updater file is TzDataCSV.csv. The TzDataCSV.csv file is created based on the tzupdater.jar file.

To set the correct time zone, you must determine the Olson Timezone area/location where the Cisco Unified CME is located and download the latest tzupdater.jar or TzDataCSV.csv to a TFTP server that is accessible to the Cisco Unified CME, such as flash or slot 0.

After a complete reboot, the phone checks if the version of its configuration file is earlier or later than 2010o. If it is earlier, the phone loads the latest tzupdater.jar and uses that updater file to calculate the Olson Timezone.

To make the Olson Timezone feature backward compatible, both the **time-zone** and **timezone** commands are retained as legacy time zones. Because the **olsontimezone** command covers approximately 500 time zones (Version 2010o of the tzupdater.jar file supports approximately 453 Olson Timezone IDs.), this command takes precedence when either the **time-zone** or the **timezone** command (that covers a total of 90 to 100 time zones only) is present at the same time as the **olsontimezone** command.

For more information on setting the time zone so that the correct local time is displayed on an IP phone, see Set Olson Timezone for SCCP Phones, on page 134 or Set Olson Timezone for SIP Phones, on page 137.

DTMF Relay

IP phones connected to Cisco Unified CME systems require the use of out-of-band DTMF relay to transport DTMF (keypad) digits across VoIP connections. The reason for this is that the codecs used for in-band transport may distort DTMF tones and make them unrecognizable. DTMF relay solves the problem of DTMF tone distortion by transporting DTMF tones out-of-band, or separate, from the encoded voice stream.

For IP phones on H.323 networks, DTMF is relayed using the H.245 alphanumeric method, which is defined by the ITU H.245 standard. This method separates DTMF digits from the voice stream and sends them as ASCII characters in H.245 user input indication messages through the H.245 signaling channel instead of the RTP channel. For information about configuring a DTMF relay in a multisite installation, see Configure DTMF Relay for H.323 Networks in Multisite Installations, on page 141.

To use remote voice-mail or IVR applications on SIP networks from Cisco Unified CME phones, the DTMF digits used by the Cisco Unified CME phones must be converted to the RFC 2833 in-band DTMF relay mechanism used by SIP phones. The SIP DTMF relay method is needed in the following situations:

- When SIP is used to connect a Cisco Unified CME system to a remote SIP-based IVR or voice-mail application.
- When SIP is used to connect a Cisco Unified CME system to a remote SIP-PSTN voice gateway that goes through the PSTN to a voice-mail or IVR application.

The requirement for 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 use voice mail on a SIP network that connects to a Cisco Unity Express system, which uses a nonstandard SIP Notify format, the DTMF digits used by the Cisco Unified CME phones must be converted to the Notify format. Additional configuration may be required for backward compatibility with Cisco CME 3.0 and 3.1. For configuration information about enabling DTMF relay for SIP networks, see Configure SIP Trunk Support, on page 142.

SIP Register Support

SIP register support enables a SIP gateway to register E.164 numbers with a SIP proxy or SIP registrar, similar to the way that H.323 gateways can register E.164 numbers with a gatekeeper. SIP gateways allow registration of E.164 numbers to a SIP proxy or registrar on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) for local SCCP phones.

When registering E.164 numbers in dial peers with an external registrar, you can also register them with a secondary SIP proxy or registrar to provide redundancy. The secondary registration can be used if the primary registrar fails.

Note No commands allow registration between the H.323 and SIP protocols.

By default, SIP gateways do not generate SIP Register messages, so the gateway must be configured to register the gateway's E.164 telephone numbers with an external SIP registrar. For information about configuring the SIP gateway to register phone numbers with Cisco Unified CME, see Configure SIP Trunk Support, on page 142.

Note When you configure SIP on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.

Define Network Parameters

Enable Calls in Your VoIP Network

Restriction

- SIP endpoints are not supported on H.323 trunks. SIP endpoints are supported on SIP trunks only.
- Cisco Unified CME 3.4 and later versions support Media Flow-through mode only; enabling SIP-to-SIP calls is required before you can successfully make SIP-to-SIP calls.
- Media Flow-around configured with the **media flow-around** command is not supported by Cisco Unified CME with SIP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections** *from-type* **to** *to-type*
5. **sip**
6. **registrar server** [**expires** [**max** *sec*] [**min** *sec*]]
7. **exit**
8. **sip-ua**
9. **notify telephone-event max-duration** *time*
10. **registrar** {**dns:***host-name* | **ipv4:***ip-address*} **expires** *seconds* [**tcp**] [**secondary**]
11. **retry register** *number*
12. **timers register** *time*
13. **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.

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode and specifies Voice over IP (VoIP) encapsulation.

Step 4	**allow-connections** *from-type* **to** *to-type*
	
	Example:
	`Router(config-voi-srv)# allow-connections h323 to h323`
	`Router(config-voi-srv)# allow-connections h323 to SIP`
	`Router(config-voi-srv)# allow-connections SIP to SIP`
		Enables calls between specific types of endpoints in a VoIP network.
		• A separate allow-connections command is required for each type of endpoint to be supported.

Step 5	**sip** **Example:** `Router(config-voi-srv)# sip`	(Optional) Enters SIP configuration mode. • Required if you are connecting IP phones running SIP directly in Cisco CME 3.4 and later.
Step 6	**registrar server** [**expires** [**max** *sec*] [**min** *sec*]] **Example:** `Router(config-voi-sip)# registrar server expires max 600 min 60`	(Optional) Enables SIP registrar functionality in Cisco Unified CME. • Required if you are connecting IP phones running SIP directly in Cisco CME 3.4 and later. **Note** Cisco Unified CME does not maintain a persistent database of registration entries across reloads. Because SIP phones do not use a keepalive functionality, the SIP phones must register again. To decrease the amount of time after which the SIP phones register again, we recommend that you change the expiry. • **max** *sec*—(Optional) Range: 600 to 86400. Default: 3600. Recommended value: 600. **Note** Ensure that the registration expiration timeout is set to a value smaller than the TCP connection aging timeout to avoid disconnection from the TCP. • **min** *sec*—(Optional) Range: 60 to 3600. Default: 60.
Step 7	**exit** **Example:** `Router(config-voi-sip)# exit`	Exits dial-peer configuration mode.
Step 8	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 9	**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*—Range: 500 to 3000. Default: 2000.
Step 10	**registrar** {**dns:***host-name* | **ipv4:***ip-address*} **expires** *seconds* [**tcp**] [**secondary**] **Example:** `Router(config-sip-ua)# registrar ipv4:10.8.17.40 expires 3600 secondary`	Registers E.164 numbers on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) with an external SIP proxy or SIP registrar server.
Step 11	**retry register** *number* **Example:** `Router(config-sip-ua)# retry register 10`	Sets the total number of SIP Register messages that the gateway should send. • *number*—Number of Register message retries. Range: 1 to 10. Default: 10.
Step 12	**timers register** *time* **Example:** `Router(config-sip-ua)# timers register 500`	Sets how long the SIP user agent (UA) waits before sending Register requests. • *time*—Waiting time, in milliseconds. Range: 100 to 1000. Default: 500.
Step 13	**end** **Example:** `Router(config-sip-ua)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure DHCP

To set up DHCP service for your DHCP clients, perform only one of the following procedures:

- If your Cisco Unified CME router is the DHCP server and you can use a single shared address pool for all your DHCP clients, see Configure Single DHCP IP Address Pool, on page 127.
- If your Cisco Unified CME router is the DHCP server and you need separate pools for each IP phone and each non-IP-phone DHCP client, see Configure Separate DHCP IP Address Pool for Each DHCP Client, on page 129.
- If the Cisco Unified CME router is not the DHCP server and you want to relay DHCP requests from IP phones to a DHCP server on a different router, see Configure DHCP Relay, on page 131.

Configure Single DHCP IP Address Pool

To create a shared pool of IP addresses for all DHCP clients, perform the following step.

Note Do *not* perform this task if you already have a DHCP server on the LAN that can be used to provide addresses to the Cisco Unified CME phones. See Enable Network Time Protocol, on page 133.

Restriction A single DHCP IP address pool cannot be used if non-IP-phone clients, such as PCs, must use a different TFTP server address.

Before You Begin

Your Cisco Unified CME router is a DHCP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *ip-address* [*mask* | / *prefix-length*]
5. **option 150 ip** *ip-address*
6. **default-router** *ip-address*
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	**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 4	**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 to be configured.

	Command or Action	Purpose
Step 5	**option 150 ip** *ip-address* **Example:** `Router(config-dhcp)# option 150 ip 10.0.0.1`	Specifies the TFTP server address from which the Cisco Unified IP phone downloads the image configuration file. • This is your Cisco Unified CME router's address.
Step 6	**default-router** *ip-address* **Example:** `Router(config-dhcp)# default-router 10.0.0.1`	(Optional) Specifies the router that the IP phones will use to send or receive IP traffic that is external to their local subnet. • If the Cisco Unified CME router is the only router on the network, this address should be the Cisco Unified CME IP source address. This command can be omitted if IP phones need to send or receive IP traffic only to or from devices on their local subnet. • The IP address that you specify for default router will be used by the IP phones for fallback purposes. If the Cisco Unified CME IP source address becomes unreachable, IP phones will attempt to register to the address specified in this command.
Step 7	**end** **Example:** `Router(config-dhcp)# end`	Returns to privileged EXEC mode.

What to Do Next

- If you are configuring Cisco Unified CME for the first time on this router, you are ready to configure NTP for the Cisco Unified CME router. For more information, see Enable Network Time Protocol, on page 133.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see Configuration Files for Phones, on page 387.

Configure Separate DHCP IP Address Pool for Each DHCP Client

To create a DHCP IP address pool for each DHCP client, including non-IP-phone clients such as PCs, perform the following steps.

Note Do *not* perform this task if you already have a DHCP server on the LAN that can be used to provide addresses to the Cisco Unified CME phones. See Enable Network Time Protocol, on page 133.

Restriction To use a separate DHCP IP address pool for each DHCP client, make an entry for each IP phone.

Before You Begin

Your Cisco Unified CME router is a DHCP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **host** *ip-address subnet-mask*
5. **client-identifier** *mac-address*
6. **option 150 ip** *ip-address*
7. **default-router** *ip-address*
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	**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 4	**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 get.
Step 5	**client-identifier** *mac-address* **Example:** `Router(config-dhcp)# client-identifier 01238.380.3056`	Specifies the MAC address of the phone, which is printed on a label on each Cisco Unified IP phone. • A separate client-identifier command is required for each DHCP client. • Add “01” prefix number before the MAC address.

	Command or Action	Purpose
Step 6	**option 150 ip** *ip-address* **Example:** `Router(config-dhcp)# option 150 ip 10.0.0.1`	Specifies the TFTP server address from which the Cisco Unified IP phone downloads the image configuration file. • This is your Cisco Unified CME router's address.
Step 7	**default-router** *ip-address* **Example:** `Router(config-dhcp)# default-router 10.0.0.1`	(Optional) Specifies the router that the IP phones will use to send or receive IP traffic that is external to their local subnet. • If the Cisco Unified CME router is the only router on the network, this address should be the Cisco Unified CME IP source address. This command can be omitted if IP phones need to send or receive IP traffic only to or from devices on their local subnet. • The IP address that you specify for default router will be used by the IP phones for fallback purposes. If the Cisco Unified CME IP source address becomes unreachable, IP phones will attempt to register to the address specified in this command.
Step 8	**end** **Example:** `Router(config-dhcp)# end`	Returns to privileged EXEC mode.

What to Do Next

- If you are configuring Cisco Unified CME for the first time on this router, you are ready to configure NTP for the Cisco Unified CME router. See Enable Network Time Protocol, on page 133.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see Configuration Files for Phones, on page 387.

Configure DHCP Relay

To set up DHCP relay on the LAN interface where the Cisco Unified IP phones are connected and enable the DHCP relay to relay requests from the phones to the DHCP server, perform the following steps.

Restriction The Cisco Unified CME router cannot be the DHCP server.

Before You Begin

There is a DHCP server that is not on this Cisco Unified CME router on the LAN that can provide addresses to the Cisco Unified CME phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service dhcp**
4. **interface** *type number*
5. **ip helper-address** *ip -address*
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	**service dhcp** **Example:** `Router(config)# service dhcp`	Enables the Cisco IOS DHCP server feature on the router.
Step 4	**interface** *type number* **Example:** `Router(config)# interface vlan 10`	Enters interface configuration mode for the specified interface.
Step 5	**ip helper-address** *ip -address* **Example:** `Router(config-if)# ip helper-address 10.0.0.1`	Specifies the helper address for any unrecognized broadcast for TFTP server and DNS server requests. • A separate **ip helper-address** command is required for each server 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 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

What to Do Next

- If you are configuring Cisco Unified CME for the first time on this router, you are ready to configure NTP for the Cisco Unified CME router. See Enable Network Time Protocol, on page 133.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see Configuration Files for Phones, on page 387.

Enable Network Time Protocol

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock timezone** *zone hours-offset* [*minutes-offset*]
4. **clock summer-time** *zone* **recurring** [*week day month hh***:***mm week day month hh***:***mm* [*offset*]]
5. **ntp server** *ip-address*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**clock timezone** *zone hours-offset* [*minutes-offset*] **Example:** `Router(config)# clock timezone pst -8`	Sets the local time zone.
Step 4	**clock summer-time** *zone* **recurring** [*week day month hh***:***mm week day month hh***:***mm* [*offset*]] **Example:** `Router(config)# clock summer-time pdt recurring`	(Optional) Specifies daylight savings time. • Default: summer time is disabled. If the **clock summer-time** *zone* **recurring** command is specified without parameters, the summer time rules default to United States rules. Default of the *offset* argument is 60.

	Command or Action	Purpose
Step 5	**ntp server** *ip-address* **Example:** `Router(config)# ntp server 10.1.2.3`	Synchronizes software clock of router with the specified NTP server.
Step 6	**exit** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

What to Do Next

- If you are configuring Cisco Unified CME for the first time on this router and if you have a multisite installation, you are ready to configure a DTMF relay. See Configure DTMF Relay for H.323 Networks in Multisite Installations, on page 141.
- If Cisco Unified CME will interact with a SIP Gateway, you must set up support for the gateway. See Configure SIP Trunk Support, on page 142.
- If you are configuring Cisco Unified CME for the first time on this router and you are ready to configure system parameters. See System-Level Parameters, on page 149.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see Configuration Files for Phones, on page 387.

Set Olson Timezone for SCCP Phones

To set the Olson Timezone so that the correct local time is displayed on a Cisco Unified SCCP IP phone, perform the following steps.

Before You Begin

- TzDataCSV.csv file is added to the configuration files of Cisco Unified 6921, 6941, 6945, and 6961 SCCP IP phones.
- tzupdater.jar file is added to the configuration files of Cisco Unified 7961 SCCP IP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tftp-server** *device:* **tzupdater.jar**
4. **tftp-server** *device:* **TZDataCSV.csv**
5. **telephony-service**
6. **olsontimezone** *timezone* **version** *number*
7. **create cnf-files**
8. **time-zone** *number*
9. **exit**
10. **clock timezone** *zone hours-offset*
11. **clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm*
12. **exit**
13. **clock set** *hh:mm:ss day month year*
14. **configure terminal**
15. **telephony-service**
16. **reset**
17. **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	**tftp-server** *device:* **tzupdater.jar** **Example:** `Router(config)# tftp-server flash:tzupdater.jar`	Enables access to the tzupdater.jar file on the TFTP server. • *device*—TFTP server that is accessible to the Cisco Unified CME, such as flash or slot 0.
Step 4	**tftp-server** *device:* **TZDataCSV.csv** **Example:** `Router(config)# tftp-server flash:TZDataCSV.csv`	Enables access to the TZDataCSV.csv file on the TFTP server. • *device*—TFTP server that is accessible to the Cisco Unified CME, such as flash or slot 0.

	Command or Action	Purpose
Step 5	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 6	**olsontimezone** *timezone* **version** *number* **Example:** `Router(config-telephony)# olsontimezone America/Argentina/Buenos Aires version 2010o`	Sets the Olson Timezone so that the correct local time is displayed on Cisco Unified SCCP IP phones or Cisco Unified SIP IP phones. • *timezone*—Olson Timezone names, which include the area (name of continent or ocean) and location (name of a specific location within that region, usually cities or small islands). • **version** *number*—Version of the tzupdater.jar or TzDataCSV.csv file. The version indicates whether the file needs to be updated or not. **Note** In Cisco Unified CME 9.0, the latest version is 2010o.
Step 7	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds the eXtensible Markup Language (XML) configuration files that are required for Cisco Unified SCCP IP phones in Cisco Unified CME.
Step 8	**time-zone** *number* **Example:** `Router(config-telephony)# time-zone 21`	Sets the time zone so that the correct local time is displayed on Cisco Unified SCCP IP phones. • *number*—Numeric code for a named time zone.
Step 9	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 10	**clock timezone** *zone hours-offset* **Example:** `Router(config)# clock timezone CST -6`	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*—Hours difference from UTC.
Step 11	**clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm* **Example:** `Router(config)# clock summer-time CST date 12 October 2010 2:00 26 April 2011 2:00`	(Optional) Configures the Cisco Unified CME system to automatically switch to summer time (daylight saving time). • *zone*—Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect. The length of the zone argument is limited to 7 characters. • **date**—Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.

	Command or Action	Purpose
		• *date*—Date of the month (1 to 31). • *month*—Month (January, February, and so on). • *year*—Year (1993 to 2035). • *hh:mm*—Time (24-hour format) in hours and minutes.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 13	**clock set** *hh:mm:ss day month year* **Example:** `Router# clock set 19:29:00 13 May 2011`	Manually sets the system software clock. • *hh:mm:ss*—Current time in hours (24-hour format), minutes, and seconds. • *day*—Current day (by date) in the month. • *month*—Current month (by name). • *year*—Current year (no abbreviation).
Step 14	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 15	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 16	**reset** **Example:** `Router(config-telephony)# reset`	Performs a complete reboot of Cisco Unfiied SCCP IP phones associated with a Cisco Unified CME router.
Step 17	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

Set Olson Timezone for SIP Phones

To set the Olson Timezone so that the correct local time is displayed on a Cisco Unified SIP IP phone, perform the following steps.

Before You Begin

- TzDataCSV.csv file is added to the configuration files of Cisco Unified 3911, 3951, 6921, 6941, 6945, and 6961 SIP IP phones.
- tzupdater.jar file is added to the configuration files of Cisco Unified 7961 SIP IP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tftp-server** *device*: **tzupdater.jar**
4. **tftp-server** *device*: **TZDataCSV.csv**
5. **voice register global**
6. **olsontimezone** *timezone* **version** *number*
7. **create profile**
8. **timezone** *number*
9. **exit**
10. **clock timezone** *zone hours-offset*
11. **clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm*
12. **exit**
13. **clock set** *hh:mm:ss day month year*
14. **configure terminal**
15. **voice register global**
16. **reset**
17. **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	**tftp-server** *device*: **tzupdater.jar** **Example:** `Router(config)# tftp-server slot0:tzupdater.jar`	Enables access to the tzupdater.jar file on the TFTP server. • *device*—TFTP server that is accessible to the Cisco Unified CME, such as flash or slot 0.
Step 4	**tftp-server** *device*: **TZDataCSV.csv**	Enables access to the TZDataCSV.csv file on the TFTP server.

	Command or Action	Purpose
	Example: `Router(config)# tftp-server slot0:TZDataCSV.csv`	• *device*—TFTP server that is accessible to the Cisco Unified CME, such as flash or slot 0.
Step 5	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 6	**olsontimezone** *timezone* **version** *number* **Example:** `Router(config-register-global)# olsontimezone America/Argentina/Buenos Aires version 2010o`	Sets the Olson Timezone so that the correct local time is displayed on Cisco Unified SCCP IP phones or Cisco Unified SIP IP phones. • *timezone*—Olson Timezone names, which include the area (name of continent or ocean) and location (name of a specific location within that region, usually cities or small islands). • **version** *number*—Version of the tzupdater.jar or tzdatacsv.csv file. The version indicates whether the file needs to be updated or not. **Note** In Cisco Unified CME 9.0, the latest version is 2010o.
Step 7	**create profile** **Example:** `Router(config-register-global)# create profile`	Generates the configuration profile files required for Cisco Unified SIP IP phones.
Step 8	**timezone** *number* **Example:** `Router(config-register-global)# timezone 21`	Sets the time zone used for Cisco Unified SIP IP phones. • *number*—Range is 1 to 53. Default is 5, Pacific Standard/Daylight Time.
Step 9	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global configuration mode.
Step 10	**clock timezone** *zone hours-offset* **Example:** `Router(config)# clock timezone CST -6`	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*—Hours difference from UTC.
Step 11	**clock summer-time** *zone* **date** *date month year hh:mm date month year hh:mm*	(Optional) Configures the Cisco Unified CME system to automatically switch to summer time (daylight saving time).

	Command or Action	Purpose
	Example: `Router(config)# clock summer-time CST date 12 October 2010 2:00 26 April 2011 2:00`	• *zone*—Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect. The length of the zone argument is limited to 7 characters. • **date**—Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command. • *date*—Date of the month (1 to 31). • *month*—Month (January, February, and so on). • *year*—Year (1993 to 2035). • *hh:mm*—Time (24-hour format) in hours and minutes.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 13	**clock set** *hh:mm:ss day month year* **Example:** `Router# clock set 15:25:00 17 November 2011`	Manually sets the system software clock. • *hh:mm:ss*—Current time in hours (24-hour format), minutes, and seconds. • *day*—Current day (by date) in the month. • *month*—Current month (by name). • *year*—Current year (no abbreviation).
Step 14	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 15	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 16	**reset** **Example:** `Router(config-register-global)# reset`	Performs a complete reboot of Cisco Unified SIP phones associated with a Cisco Unified CME router.
Step 17	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Configure DTMF Relay for H.323 Networks in Multisite Installations

To configure DTMF relay for H.323 networks in a multisite installation only, perform the following steps.

Note To configure DTMF relay on SIP networks, see Configure SIP Trunk Support, on page 142.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **dtmf-relay h245-alphanumeric**
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* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode.
Step 4	**dtmf-relay h245-alphanumeric** **Example:** `Router(config-dial-peer)# dtmf-relay h245-alphanumeric`	Specifies the H.245 alphanumeric method for relaying dual tone multifrequency (DTMF) tones between telephony interfaces and an H.323 network.
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

What to Do Next

- To set up support for a SIP trunk, see Configure SIP Trunk Support, on page 142.

- If you are configuring Cisco Unified CME for the first time on this router and you are ready to configure system parameters. For more information, see System-Level Parameters, on page 149.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see Configuration Files for Phones, on page 387.

Configure SIP Trunk Support

To enable DTMF relay on a dial-peer for a SIP gateway and set up the gateway to register phone numbers with Cisco Unified CME, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **dtmf-relay rtp-nte**
5. **dtmf-relay sip-notify**
6. **exit**
7. **sip-ua**
8. **notify telephone-event max-duration** *msec*
9. **registrar** {**dns:** *host-name* | **ipv4:** *ip-address*} **expires** *seconds* [**tcp**] [**secondary**]
10. **retry register** *number*
11. **timers register** *msec*
12. **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* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode.

	Command or Action	Purpose
Step 4	**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 and enables DTMF relay using the RFC 2833 standard method.
Step 5	**dtmf-relay sip-notify** **Example:** `Router(config-dial-peer)# dtmf-relay sip-notify`	Forwards DTMF tones using SIP NOTIFY messages.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.
Step 7	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 8	**notify telephone-event max-duration** *msec* **Example:** `Router(config-sip-ua)# notify telephone-event max-duration 2000`	Sets the maximum milliseconds allowed between two consecutive NOTIFY messages for a single DTMF event. • **max-duration** *time*—Range: 500 to 3000. Default: 2000.
Step 9	**registrar** {**dns:** *host-name* | **ipv4:** *ip-address*} **expires** *seconds* [**tcp**] [**secondary**] **Example:** `Router(config-sip-ua)# registrar ipv4:10.8.17.40 expires 3600 secondary`	Registers E.164 numbers on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) with an external SIP proxy or SIP registrar server.
Step 10	**retry register** *number* **Example:** `Router(config-sip-ua)# retry register 10`	Sets the total number of SIP Register messages that the gateway should send. • *number*—Number of Register message retries. Range: 1 to 10. Default: 10.
Step 11	**timers register** *msec* **Example:** `Router(config-sip-ua)# timers register 500`	Sets how long the SIP user agent (UA) waits before sending Register requests. • *time*—Waiting time, in milliseconds. Range: 100 to 1000. Default: 500.
Step 12	**end** **Example:** `Router(config-sip-ua)# end`	Returns to privileged EXEC mode.

Verify SIP Trunk Support Configuration

To verify SIP trunk configuration, perform the following steps in any order.

Step 1 **show sip-ua status**

Use this command to display the time interval between consecutive NOTIFY messages for a telephone event. In the following example, the time interval is 2000 ms:

Example:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP User Agent bind status(signaling):DISABLED

SIP User Agent bind status(media):DISABLED

SIP 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
```

Step 2 **show sip-ua timers**

This command displays the waiting time before Register requests are sent; that is, the value that has been set with the **timers register** command.

Step 3 **show sip-ua register status**

This command displays the status of local E.164 registrations.

Step 4 **show sip-ua statistics**

This command displays the Register messages that have been sent.

Change the TFTP Address on a DHCP Server

To change the TFTP IP address after it has already been configured, perform the following steps.

Restriction If the DHCP server is on a different router than Cisco Unified CME, reconfigure the external DHCP server with the new IP address of the TFTP server.

Before You Begin

Your Cisco Unified CME router is a DHCP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **option 150 ip** *ip-address*
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	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool pool2`	Enters DHCP pool configuration mode to create or modify a DHCP pool. • *pool-name*—Previously configured unique identifier for the pool to be configured.
Step 4	**option 150 ip** *ip-address* **Example:** `Router(config-dhcp)# option 150 ip 10.0.0.1`	Specifies the TFTP server IP address from which the Cisco Unified IP phone downloads the image configuration file, XmlDefault.cnf.xml.
Step 5	**end** **Example:** `Router(config-dhcp)# end`	Returns to privileged EXEC mode.

Configuration Examples for Network Parameters

NTP Server

The following example defines the pst timezone as 8 hours offset from UTC, using a recurring daylight savings time called pdt, and synchronizes the clock with the NTP server at 10.1.2.3:

```
clock timezone pst -8
clock summer-time pdt recurring
ntp server 10.1.2.3
```

DTMF Relay for H.323 Networks

The following excerpt from the **show running-config** command output shows a dial peer configured to use H.245 alphanumeric DTMF relay:

```
dial-peer voice 4000 voip
 destination-pattern 4000
 session target ipv4:10.0.0.25
 codec g711ulaw
 dtmf-relay h245-alphanumeric
```

Where to Go Next

- If you are configuring Cisco Unified CME for the first time on this router, you are ready to configure system-level parameters. See System-Level Parameters, on page 149.
- If you modified network parameters for an already configured Cisco Unified CME router, you are ready to generate the configuration file to save the modifications. See Configuration Files for Phones, on page 387.

Feature Information for Network Parameters

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

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

Table 9: Feature Information for Network Parameters

Feature Name	Cisco Unified CME Version	Modification
Olson Timezone	9.0	Eliminates the need to update time zone commands or phone loads to accommodate a new country with a new time zone or an existing country whose city or state wants to change their time zone, using the **olsontimezone** command in either telephony-service or voice register global configuration mode.

CHAPTER 6

System-Level Parameters

Prerequisites for System-Level Parameters

- To directly connect Cisco Unified IP phones that are running Session Initiation Protocol (SIP) in Cisco Unified CME, Cisco CME 3.4 or a later version must be installed on the router. For installation information, see Install and Upgrade Cisco Unified CME Software, on page 101.
- Cisco Unified CME must be configured to work with your IP network. For configuration information, see Network Parameters, on page 121.

Information About Configuring System-Level Parameters

Bulk Registration Support for SIP Phones

Cisco Unified CME 8.6 enhances the bulk registration feature for Cisco Unified SIP IP phones by optimizing the two main transactions involved in bulk registration process and minimizing the number of required messages to be sent to the phones. The bulk registration process involves the following two main transactions:

- Register—Register transaction handles per line REGISTER messages coming to Cisco Unified CME and provisions phone DNs by creating dialpeers and various phone data structures.
- Phone Status Update—Phone status update transaction sends back device information using REFER and NOTIFY messages.

In Cisco Unified CME 8.6, the bulk registration process consists of only one REGISTER message per phone instead of one REGISTER message per phone per line, thus reducing any negative impact on your router's performance. For information on configuring bulk registration, see Configure Bulk Registration for SIP IP Phones, on page 174.

The **show voice register pool** command displays the registration method a phone uses: per line, bulk-in progress, or bulk-completed. The per line option indicates that the phone is using the per line registration process. The bulk-in progress option indicates that the phone is using the bulk registration process but the registration process is not complete yet. The bulk-completed option indicates that the phone is registered using the bulk registration process and the registration process is complete. For information on verifying the phone registration process, see Verify Phone Registration Type and Status, on page 175.

Note The bulk registration feature in Cisco Unified CME 8.6 optimizes line registration on SIP phones and is a phone interop feature. The bulk registration feature is not related to the **bulk** command under voice register global configuration mode.

In earlier versions of Cisco Unified CME, the registration process was very lengthy and several SIP messages were exchanged between the end points and Cisco Unified CME to properly provision the phone.

Table 10: Number of Messages Required for an Eight-Button IP Phone, on page 150 lists the number of messages required to register an eight-button Cisco Unified SIP IP phone, where all of the eight buttons can be configurd as a shared line with message waiting indicator (MWI) notification enabled, to Cisco Unified CME.

Table 10: Number of Messages Required for an Eight-Button IP Phone

Transactions	Method	Messages Per Transaction	Number of Transactions	Total number of messages (per line)	Total number of messages (bulk)
Register	REGISTER	2	8	24	3
Phone Status Update	REFER remotecc NOTIFY (mwi, service-control)	2 2	3 8	6 16	2
Subscription	SUBSCRIBE (sharedline)	4	8	32	32
Total				78	37

You can see from the preceding table that more than 70 messages are required to register one 8-button IP phone. If there is a simultaneous registration of more phones, the amount of messages can be overwhelming and can have a negative impact on the performance of the router.

With the enhanced bulk registration process, the two main transactions (Register and Phone Status Update) are optimized to minimize the number of messages required to complete the phone registration process. Table 10: Number of Messages Required for an Eight-Button IP Phone, on page 150 shows that the total number of messages required for bulk registration is only 37.

Register Transaction

The following is an example of the REGISTER message:

```
REGISTER sip:28.18.88.1 SIP/2.0

Via: SIP/2.0/TCP 28.18.88.33:44332;branch=z9hG4bK53f227fc

From: <sip:6010@28.18.88.1>;tag=001b2a893698027db8ea0454-26b9fb0c

To: <sip:6010@28.18.88.1>

Call-ID: 001b2a89-3698011e-280209a4-567e339c@28.18.88.33

Max-Forwards: 70

Date: Wed, 03 Mar 2010 01:18:34 GMT

CSeq: 240 REGISTER

User-Agent: Cisco-CP7970G/8.4.0

Contact: <sip:6010@28.18.88.33:44332;transport=tcp >
;+sip.instance="<urn:uuid:00000000-0000-0000-0000-001b2a893698 >
";+u.sip!model.ccm.cisco.com="30006"

Supported:
replaces,join,norefersub,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,
X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-3.0.0,X-cisco-xsi-7.0.1

Reason: SIP;cause=200;text="cisco-alarm:23 Name=SEP001B2A893698 Load=SIP70.8-4-2-30S
Last=reset-restart"

Expires: 3600

Content-Type: multipart/mixed; boundary=uniqueBoundary

Mime-Version: 1.0

Content-Length: 982

--uniqueBoundary

Content-Type: application/x-cisco-remotecc-request+xml

Content-Disposition: session;handling=optional


>

 < x-cisco-remotecc-request >

<bulkregisterreq >

 < contact all="true" >

 < register >  < /register >

 < /contact >

 < /bulkregisterreq >

 < /x-cisco-remotecc-request >


--uniqueBoundary

Content-Type: application/x-cisco-remotecc-request+xml

Content-Disposition: session;handling=optional
```

```
 >
 < x-cisco-remotecc-request >
  < optionsind >
   < combine max="6" >
    < remotecc >
     < status >  < /status >
    < /remotecc >
    < service-control >  < /service-control >
   < /combine >
   < dialog usage="hook status" >
    < unot >  < /unot >
    < sub >  < /sub >
   < /dialog >
   < dialog usage="shared line" >
    < unot >  < /unot >
    < sub >  < /sub >
   < /dialog >
   < presence usage="blf speed dial" >
    < unot >  < /unot >
    < sub >  < /sub >
   < /presence >
   < joinreq >  < /joinreq >
  < /optionsind >
 < /x-cisco-remotecc-request >

--uniqueBoundary--
```

The following is an example of a response to the preceding REGISTER message:

```
SIP/2.0 200 OK
Date: Wed, 03 Mar 2010 01:18:41 GMT
From:  < sip:6010@28.18.88.1 > ;tag=001b2a893698027db8ea0454-26b9fb0c
Content-Length: 603
To:  < sip:6010@28.18.88.1 > ;tag=E2556C-6C1
Contact:  < sip:6010@28.18.88.33:44332;transport=tcp > ;expires=3600;x-cisco-newreg
Expires:  3600
Content-Type: multipart/mixed;boundary=uniqueBoundary
Call-ID: 001b2a89-3698011e-280209a4-567e339c@28.18.88.33
Via: SIP/2.0/TCP 28.18.88.33:44332;branch=z9hG4bK53f227fc
```

```
Server: Cisco-SIPGateway/IOS-12.x

CSeq: 240 REGISTER

Mime-Version: 1.0

  >  < x-cisco-remotecc-response >  < response >  < code > 200 < /code >  < optionsind >
< combine max="6" >  < remotecc >
  < status/ >  < /remotecc >  < service-control/ >  < /combine >  < dialog usage="shared
line" >  < sub/ >  < /dialog >
< presence usage="blf speed dial" >  < sub/ >  < /presence >  < /optionsind >  < /response
 >  < /x-cisco-remotecc-response >
```

Phone Status Update Transaction

Cisco Unified IP phones use the option indication to negotiate supported options with Cisco Unified CME via remotecc request. Cisco Unified CME selects an option or options that it wishes to support and return it in the response. Cisco Unified CME ignores items (elements, attributes, and values) that it fails to understand. A new phone option, combine, is defined to optimize phone status update. This option combines remotecc status information (cfwdall, privacy, dnd, bulk mwi) and service-control. The following is an example of a combined status update:

```
<optionsind>
<combine max="5">
<remotecc><status/></remotecc>
<service-control/>
</combine>
</optionsind>
```

The following is another example of a combined status update:

```
<optionsind>
<combine max="4">
<remotecc><status/></remotecc>
<service-control/>
</combine>
</optionsind>
```

To minimize the data size, Cisco Unified CME and the phone agree ahead of time on a default value to apply updates. Therefore, during initial registration, Cisco Unified CME will not send the value if it matches the agreed upon default. Table 11: Status Information and Default, on page 153 captures the existing status information and applicable default value.

Table 11: Status Information and Default

Status	Default	Initialization
CallForwardAll Update	No default	Always send regardless of the value
Privacyrequest	Disabled	Only send if the value is not equal to the default
DnDupdate	Disabled	Only send if value is not equal to the default
Bulkupdate (MWI)	No default	Always send regardless of value

During bulk registration, Cisco Unified CME uses a single REFER message to send combined phone status update message for phone status updates such as cfwdallupdate, privacyrequet, DnDupdate, and Bulkupdate (MWI) instead of sending phone status in individual NOTIFY or REFER message to the phone. The following is an example of the single REFER message sent by Cisco Unified CME to the phone:

```
REFER sip:6010@28.18.88.33:44332 SIP/2.0
Content-Id: <1483336>
From: <sip:28.18.88.1>;tag=E256D4-2316
Timestamp: 1267579121
Content-Length: 934
User-Agent: Cisco-SIPGateway/IOS-12.x
Require: norefersub
Refer-To: cid:1483336
To: <sip:6010@28.18.88.33>
Contact: <sip:28.18.88.1:5060>
Referred-By: <sip:28.18.88.1>
Content-Type: multipart/mixed;boundary=uniqueBoundary
Call-ID: 89CBE590-259911DF-80589501-4E753388@28.18.88.1
Via: SIP/2.0/UDP 28.18.88.1:5060;branch=z9hG4bKA22639
CSeq: 101 REFER
Max-Forwards: 70
Mime-Version: 1.0

 --uniqueBoundary
 Content-Type: application/x-cisco-remotecc-request+xml

<x-cisco-remotecc-request>
<cfwdallupdate><fwdaddress></fwdaddress><tovoicemail>off</tovoicemail></cfwdallupdate></x-cisco-remotecc-request>



--uniqueBoundary
Content-Type: application/x-cisco-remotecc-request+xml



<x-cisco-remotecc-request>
<privacyreq><status>true</status></privacyreq>
</x-cisco-remotecc-request>
--uniqueBoundary
Content-Type: application/x-cisco-remotecc-request+xml


<x-cisco-remotecc-request>
<bulkupdate>
<contact all="true"><mwi>no</mwi></contact>
<contact line=" 1"><mwi>yes</mwi></contact>
<contact line=" 3"><mwi>yes</mwi></contact>
</bulkupdate>
</x-cisco-remotecc-request>


--uniqueBoundary
Content-Type: text/plain
action=check-version
RegisterCallId={001b2a89-3698011e-280209a4-567e339c@28.18.88.33}
ConfigVersionStamp={0106514225374329}
DialplanVersionStamp={}
SoftkeyVersionStamp={0106514225374329}

--uniqueBoundary--
```

Note Cisco Unified IP phones use the TCP for registration refresh. TCP socket has a default keepalive time out session of 60 minutes. If registration refresh to Cisco Unified CME does not takes place within an hour (60 minutes), the TCP connection will be removed. This will make the phones restart instead of refresh. To stop the phones from restarting, adjust the registrar expire timer under voice service voip or set the timer connection aging under sip-ua to a value greater than what the phone uses for registration refreshes. For example, if the phone does a registration refresh every 60 minutes, then setting up a timer connection aging to 100 minutes will guarantee that the TCP keeps the connection open. Or you can set the registrar expire maximum value to less than 3600.

DSCP

Differentiated Services Code Point (DSCP) packet marking is used to specify the class of service for each packet. Cisco Unified IP Phones get their DSCP information from the configuration file that is downloaded to the device.

In earlier versions of Cisco Unified CME, the DSCP value is predefined. In Cisco Unified CME 7.1 and later versions, you can configure the DSCP value for different types of network traffic. Cisco Unified CME downloads the configured DSCP value to SCCP and SIP phones in their configuration files and all control messages and flow-through RTP streams are marked with the configured DSCP value. This allows you to set different DSCP values, for example, for video streams and audio streams.

For configuration information, see Set Up Cisco Unified CME for SCCP Phones , on page 175 or Set Up Cisco Unified CME for SIP Phones, on page 192.

Maximum Ephones in Cisco Unified CME 4.3 and Later Versions

In Cisco Unified CME 4.3 and later versions, the **max-ephones** command is enhanced to set the maximum number of SCCP phones that can register to Cisco Unified CME, without limiting the number that can be configured. In previous versions of Cisco Unified CME, the **max-ephones** command defined the maximum number of phones that could be both configured and registered.

This enhancement expands the maximum number of phones that can be configured to 1000. The maximum number of phones that can register to Cisco Unified CME has not changed; it is dependent on the number of phones supported by the hardware platform and is limited by the **max-ephones** command.

This enhancement supports features, such as Extension Assigner, that require you to configure more phones than can register. For example, if you set the **max-ephones** command to 50 and configure 100 ephones, only 50 phones can register to Cisco Unified CME, one at a time in random order. The remaining 50 phones cannot register and an error message displays for each rejected phone. This enhancement also allows you to assign ephone tags that match the extension number of the phone, for extensions up to 1000.

If you reduce the value of the **max-ephones** command, currently registered phones are not forced to unregister until a reboot. If the number of registered phones, however, is already equal to or more than the max-ephones value, no additional phones can register to Cisco Unified CME. If you increase the value of the **max-ephones** command, the previously rejected ephones are able to register immediately until the new limit is reached.

Note For Cisco Integrated Services Router 4351, you can set the max-ephones value to 3925. For Cisco Integrated Services Router 4331, you can set the max-ephones value to 2921. For Cisco Integrated Services Router 4321, you can set the max-ephones value to 2901. For Cisco Integrated Services Router 4400 series, you can set the max-ephones value to 4451.

Network Time Protocol for SIP Phones

Although SIP phones can synchronize to a Cisco Unified CME router, the router can lose its clock after a reboot causing phones to display the wrong time. SIP phones registered to a Cisco Unified CME router can synchronize to a Network Time Protocol (NTP) server. Synchronizing to an NTP server ensures that SIP phones maintain the correct time. For configuration information, see Set Network Time Protocol for SIP Phones, on page 199.

Per-Phone Configuration Files

In Cisco Unified CME 4.0 and later versions, you can use an external TFTP server to off load the TFTP server function on the Cisco Unified CME router. Using flash memory or slot 0 memory on the Cisco Unified CME router allows you to use different configuration files for each phone type or for each phone, permitting you to specify different user locales and network locales for different phones. Before Cisco Unified CME 4.0, you could specify only a single default user and network locale for a Cisco Unified CME system.

You can specify one of the following four locations to store configuration files:

- System—This is the default. When system:/its is the storage location, there is only one default configuration file for all phones in the system. All phones, therefore, use the same user locale and network locale. User-defined locales are not supported.
- Flash or slot 0—When flash memory or slot 0 memory on the router is the storage location, you can create additional configuration files to apply per phone type or per individual phone. Up to five user and network locales can be used in these configuration files.

Note When the storage location you selected is flash memory and the file system type on this device is Class B (LEFS), you must check the free space on the device periodically and use the **squeeze** command to free the space used up by deleted files. Unless you use the **squeeze** command, the space used by the moved or deleted configuration files cannot be used by other files. Rewriting flash memory space during the squeeze operation may take several minutes. We recommend that you use this command during scheduled maintenance periods or off-peak hours.

- TFTP—When an external TFTP server is the storage location, you can create additional configuration files that can be applied per phone type or per individual phone. Up to five user and network locales can be used in these configuration files.

You can then specify one of the following ways to create configuration files:

- Per system—This is the default. All phones use a single configuration file. The default user and network locale in a single configuration file are applied to all phones in the Cisco Unified CME system. Multiple locales and user-defined locales are not supported.
- Per phone type—This setting creates separate configuration files for each phone type. For example, all Cisco Unified IP Phone 7960s use XMLDefault7960.cnf.xml, and all Cisco Unified IP Phone 7905s use XMLDefault7905.cnf.xml. All phones of the same type use the same configuration file, which is generated using the default user and network locale. This option is not supported if you store the configuration files in the system:/its location.
- Per phone—This setting creates a separate configuration file for each phone by MAC address. For example, a Cisco Unified IP Phone 7960 with the MAC address 123.456.789 creates the per-phone configuration file SEP123456789.cnf.xml. The configuration file for a phone is generated with the default user and network locale unless a different user and network locale is applied to the phone using an ephone template. This option is not supported if you store the configuration files in the system:/its location.

For configuration information, see Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.

HFS Download Support for IP Phone Firmware and Configuration Files

Legacy IP phones access the TFTP server to download firmware and configuration files but Cisco Unified CME 8.8 enhances download support for SIP phone firmware, scripts, midlets, and configuration files using the HTTP File-Fetch Server (HFS) infrastructure.

In Cisco Unified CME 8.8 and later versions, SIP phones use an HTTP server as the primary download service when it is configured and access a TFTP server as a secondary or fallback option when the HTTP server fails.

Note When the HFS download service is not configured, SIP phones automatically access the TFTP server.

The following scenario shows a successful download sequence using an HTTP server:

An IP phone initiates TCP connection to port 6970. A connection is established and an internal request for a file is sent to the HTTP server. The phone receives the HTTP response status code of 200, signifying that the download is successful.

The following scenario shows a download sequence that begins with an IP phone using an HTTP server to download files and ends with a TFTP server as a fallback option when the initial download attempt fails:

An IP phone initiates TCP connection to port 6970 but is unable to establish a connection. The phone contacts the TFTP server and sends an internal request for a file. The file is successfully downloaded from the TFTP server.

The following scenario shows how a download sequence that starts with an HTTP server does not always fall back to the TFTP server when the initial download attempt fails:

An IP phone initiates TCP connection to port 6970. A connection is established and an internal request for a file is sent to the HTTP server. The phone receives the HTTP response status code of 404, signifying that the file requested could not be found. Because the file cannot be found, the request is not sent to the TFTP server.

Note The configuration files are shared by the HTTP and TFTP servers. However, the firmware files are different for each server.

For more information on Phone Firmware Files, see Install and Upgrade Cisco Unified CME Software, on page 101.

For more information on Per-Phone Configuration Files, see Per-Phone Configuration Files, on page 156.

For more information on Configuration Files for Phones in Cisco Unified CME, see Generate Configuration Files for Phones, on page 388.

Enable HFS Service

To enable the HFS download service, the underlying HTTP server must be enabled first because the HFS infrastructure is built on top of an existing IOS HTTP server.

```
Router(config)# ip http server
```

This HFS infrastructure enables multiple HTTP services to co-exist. The HFS download service runs on custom port 6970 but can also share default port 80 with other services. Other HTTP services run on other non-standard ports like 1234.

```
Router(config)# ip http server
Router(config)# ip http port1234
```

The HFS download service starts when the following is configured in telephony-service configuration mode.

For the default port:

```
Router(config-telephony)# hfs enable
```

For the custom port:

```
Router(config-telephony)# hfs enable port 6970
```

Note If the entered custom HFS port clashes with the underlying IP HTTP port, an error message is displayed and the command is disallowed.

In the following example, port 6970 is configured as the IP HTTP port. When the HFS port is configured with the same value, an error message is displayed to show that the port is already in use.

```
Router (config)# ip http port 6970
.
.
Router (config)# telephony-service
Router (config-telephony)# hfs enable port 6970
```

Error Message Invalid port number or port in use by other application

Explanation The HFS port number is already in use by the underlying IP HTTP server.

Recommended Action Use an HFS port that is different from the underlying IP HTTP port.

Note Because IP phones are hardcoded to use port 6970 to connect to Cisco Unified CME, you must search for other applications running on port 6970 and assign them with ports different from 6970 to prevent a failure in connecting to Cisco Unified CME.

For configuration information, see Enable HFS Download Service for SIP Phones, on page 200.

File Binding and Fetching

File binding and fetching using the HTTP server can be classified into two:

- Explicit binding – The **create profile** command triggers the system to generate the configuration and firmware files and store them in RAM or a flash memory. The system asks the new internal application programming interfaces (APIs) implemented by the HFS download service to bind the filename and alias that an IP phone wants to access to their corresponding URL.
- Loose binding – The HFS download service enables the Cisco Unified CME system to configure a home path from where any requested firmware file that has no explicit binding can be searched and fetched. The files can be stored on any device (such as flash memory or NVRAM) under a root directory or a suitable subdirectory.

  No matter how the system is configured, if there is no explicit binding, the files will go to the home path.

  An advantage of the HFS service over the TFTP service is that only the absolute path where the firmware files are located needs to be configured in telephony-service configuration mode.

  For example:

  ```
  Router(config-telephony)# hfs home-path flash:/cme/loads/
  ```

  In contrast, the TFTP service requires that each file be explicitly bound to its URL using the following **tftp-server** command:

  ```
  tftp-server flash: SCCP70.8-3-3-14S.loads
  ```

  The method is inefficient because this step must be repeated for each file that needs to be fetched using the TFTP server.

For information on verifying HFS file bindings, see Example for Verifying the HFS File Bindings of Cisco Unified SIP IP Phone Configuration and Firmware Files, on page 214.

For information on how to configure the home path, see Configure HFS Home Path for SIP Phone Firmware Files, on page 202.

Locale Installer

Installing and configuring locale files in Cisco Unified CME when using an HTTP server is the same as when using a TFTP server.

For configuration information, see Use the Locale Installer in Cisco Unified CME 7.0(1) and Later Versions, on page 419.

Security Recommendations

Like any access interface, the HFS download service can open router files that should only be accessed by authorized persons. Security issues are made more severe by the fact that the HFS download service is HTTP based, enabling anyone with a simple web browser to access sensitive files, such as configuration or image files, by entering a random string of words.

However, the HFS security problem is restricted to the loose binding operation, where the administrator provides an HFS home path in which the phone firmware and other related files are stored.

In the case where a unique directory path (where only the phone firmware files are stored) is used as the HFS home path

```
(config-telephony)# hfs home-path flash:/cme/loads/
```

only those files that are in flash:/cme/loads/ can be accessed.

But when it is the root directory path that is used as the HFS home path

```
(config-telephony)# hfs home-path flash:/
```

there is a risk of making configuration files and system images, which are stored in the root directory shared with the phone firmware files, accessible to unauthorized persons.

The following are two recommendations on how to make firmware files inaccessible to unauthorized persons:

- Create a unique directory, which is not shared by any other application or used for any other purpose, fpr IP phone firmware files. Using a root directory as the HFS home path is not recommended.
- Use the **ip http access-class** command to specify the access list that should be used to restrict access to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Redundant Cisco Unified CME Router for SCCP Phones

A second Cisco Unified CME router can be configured to provide call-control services if the primary Cisco Unified CME router fails. The secondary Cisco Unified CME router provides uninterrupted services until the primary router becomes operational again.

When a phone registers to the primary router, it receives a configuration file from the primary router. Along with other information, the configuration file contains the IP addresses of the primary and secondary Cisco Unified CME routers. The phone uses these addresses to initiate a keepalive (KA) message to each router. The phone sends a KA message after every KA interval (30 seconds by default) to the router with which it is registered and after every two KA intervals (60 seconds by default) to the other router. The KA interval can be adjusted.

If the primary router fails, a phone will not receive an acknowledgment (ACK) to its KA message to the primary router. If the phone does not get an ACK from the primary router for three consecutive KAs, it registers with the secondary Cisco Unified CME router.

During the time that the phone is registered to the secondary router, it keeps sending a KA probe to the primary router to see if it has come back up, now every 60 seconds by default or two times the normal KA interval. After the primary Cisco Unified CME router returns to normal operation, the phone starts receiving ACKs for its probes. After the phone receives ACKs from the primary router for three consecutive probes, it switches back to the primary router and re-registers with it. The re-registration of phones with the primary router is also called rehoming.

The physical setup for redundant Cisco Unified CME routers is as follows. The FXO line from the PSTN is split using a splitter. From the splitter, one line goes to the primary Cisco Unified CME router and the other line goes to the secondary Cisco Unified CME router. When a call comes in on the FXO line, it is presented to both the primary and secondary Cisco Unified CME routers. The primary router is configured by default to answer the call immediately. The secondary Cisco Unified CME router is configured to answer the call after three rings. If the primary router is operational, it answers the call immediately and changes the call state so that the secondary router does not try to answer it. If the primary router is unavailable and does not answer the call, the secondary router sees the new call coming in and answers after three rings.

The secondary Cisco Unified CME router should be connected in some way on the LAN, either through the same switch or through another switch that may or may not be connected to the primary Cisco Unified CME router directly. As long as both routers and the phones are connected on the LAN with the appropriate configurations in place, the phones can register to whichever router is active.

Configure primary and secondary Cisco Unified CME routers identically, with the exception that the FXO voice port from the PSTN on the secondary router should be configured to answer after more rings than the primary router, as previously explained. The same command is used on both routers to specify the IP addresses of the primary and secondary routers.

For configuration information, see Configure Redundant Router for SCCP Phones, on page 184.

Restriction

- Due to lack of High Availability support, Stateful Swtichover or preservation of active calls is not supported in the redundancy feature offered by Unified CME.
- The physical setup for redundant Cisco Unified CME routers only support Loop start signaling. The Ground start signaling is not supported.

Redundant Cisco Unified CME Router for SIP Phones

A secondary Cisco Unified CME router can be configured to provide call-control services if the primary Cisco Unified CME router fails. The secondary Cisco Unified CME router provides uninterrupted services until the primary router becomes operational again.

When a SIP phone registers to the primary router, it receives a configuration file from the primary router. Along with other information, the configuration file contains the IP addresses of the primary and secondary Cisco Unified CME routers. The phone uses these addresses to initiate a keepalive (KA) message to the secondary CME router. The phone sends a REGISTER message to the primary router for registration and a keepalive REGISTER message with Expires=0, to the secondary router during the keepalive interval (every 120 seconds by default). The keepalive interval can be configured (Range is 120 to 65535).

If primary router fails, a SIP phone (on registration refresh) will not receive a successful response for its REGISTER message. On unsuccessful response from primary router, phone registers with the secondary router. When the phone is registered to the secondary router, phone sends keepalive REGISTER (Expires=0) messages to the primary router.

After the primary Cisco Unified CME router returns to normal operation, the phone sends a "token-registration" to the primary router seeking permission to move registration of the phone from the standby secondary router to the primary router. To obtain a token, the SIP phones sends a Out-of-Dialog REFER message to the primary router for registration. The primary router accepts the token by responding with a 202 Accepted response. When the SIP phones receive the token (202 Accepted response) from the primary router, the phones will immediately de-register from the secondary router by sending a REGISTER message with Expires=0 for each line and registers back to the primary router. The re-registration of phones with the primary router is called rehoming.

No signaling or media preservation is done for any active calls on Unified CME. Hence during failover on primary CME, calls would remain in active state. But media would not be present for those calls. The SIP phones will not register to the secondary router until the active call is disconnected.

The secondary Cisco Unified CME router is connected directly to the same SIP trunk as the primary Cisco Unified CME router. As long as both routers and the phones are connected on the LAN with the appropriate configurations in place, the phones can register to whichever router is active. You should configure the primary and secondary Cisco Unified CME routers identically. The same command is used on both routers to specify the IP addresses of the primary and secondary routers.

For configuration information, see Configure Redundant Router for SIP Phones, on page 186.

Restriction

- Due to lack of High Availability support, Stateful Swtichover or preservation of active calls is not supported in the redundancy feature offered by Unified CME.

Timeouts

The following system-level timeout parameters have default values that are generally adequate:

- Busy Timeout—Length of time that can elapse after a transferred call reaches a busy signal before the call is disconnected.
- Interdigit Timeout—Length of time that can elapse between the receipt of individual dialed digits before the dialing process times out and is terminated. If the timeout ends before the destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial-peer destination patterns (dial plans).
- Ringing Timeout—Length of time a phone can ring with no answer before returning a disconnect code to the caller. This timeout is used only for extensions that do not have no-answer call forwarding enabled. The ringing timeout prevents hung calls received over interfaces, such as FXO, that do not have forward-disconnect supervision.
- Keepalive—Interval determines how often a message is sent between the router and Cisco Unified IP phones, over the session, to ensure that the keepalive timeout is not exceeded. If no other traffic is sent over the session during the interval, a keepalive message is sent.

For configuration information, see Modify Defaults for Timeouts for SCCP Phones, on page 182.

IPv6 Support for Cisco Unified CME SCCP Endpoints

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over digital networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in Cisco Unified CME allows the network to behave transparently in a dual-stack (IPv4 and IPv6) environment and provides additional IP address space to SCCP phones and devices that are connected to the network. For information on configuring DHCP for IPv6, see Network Parameters, on page 121.

Before Cisco Unified CME 8.0, SCCP supported IPv4 addresses (4 bytes) only. With Cisco Unified CME 8.0, the SCCP version is upgraded to store IPv6 address (16 bytes) also.

The following SCCP phones and devices are supported on IPv6: 7911, 7931, 7941G, 7941GE, 7961G, 7961GE, 7970G, 7971G, 7971G-GE, 7942, 7962, 7945, 7965, 7975, SCCP analogue gateway, Xcoder, and Hardware Conference devices. For more information on configuring SCCP IP phones for IPv6 source address, see Configure IPv6 Source Address for SCCP IP Phones, on page 169.

Note You must disable Alternative Network Address Transport (ANAT) globally for SIP lines if you have a Cisco Unified CME with a dual-stack SIP trunk and enable ANAT at dial-peer level for the SIP trunk.

Support for IPv4-IPv6 (Dual-Stack)

Cisco Unified CME 8.0 can interact with and support any SCCP devices that support IPv4 only or both IPv4 and IPv6 (dual-stack). In dual-stack mode, two IP addresses are assigned to an interface, one is an IPv4 address and the other is an IPv6 address. Both IPv4 and IPv6 stacks are enabled on the voice gateways so that applications can interact with both versions of IP addresses. To support devices that use IPv4 only, IPv6 only, or both IPv4 and IPv6 (dual-stack) addresses, you must ensure that the Cisco Unified CME has both IPv4 address and IPv6 address enabled. For more information, see Configure IP Phones in IPv4, IPv6, or Dual Stack Mode, on page 167.

Media Flow Through and Flow Around

Media transport modes, such as flow around and flow through, are used to transport media packets across endpoints. Media flow around enables media packets to pass directly between the endpoints, without the intervention of the IP-IP Gateway (IPIPGW). Media flow through enables media packets to pass through the endpoints, without the intervention of the IPIPGW.

Table 12: Call Flow Scenarios Between IPv4 only, IPv6 only, and Dual-Stack, on page 163 lists media flow-through and flow-around scenarios between endpoints that support IPv4, IPv6, and dual- stack. When both endpoints are IPv4 only or IPv6 only, the call flows around. When one endpoint is IPv4 and the other is IPv6, calls flow through. When one endpoint is dual-stack and the other IPv4 or IPv6 the calls flow around. When both endpoints are dual-stack calls flow around or follows the preference (preferred IP address version) selected by protocol mode in dual-stack.

Table 12: Call Flow Scenarios Between IPv4 only, IPv6 only, and Dual-Stack

IP Versions	IPv4 Only	IPv6 Only	Dual-Stack
IPv4 Only	Flow Around [1]	Flow Through	Flow Around
IPv6 Only	Flow Through	Flow Around	Flow Around/IPv6
Dual-Stack	Flow Around/IPv4	Flow Around/IPv6	Flow Around/Preference

1 When MTP is configured under ephones all the call flow-around scenarios change to flow-through. This is also applicable to cross-VRF endpoints.

Media Flow Around Support for SIP-SIP Trunk Calls

Cisco Unified CME 8.5 and later versions support the media flow around functionality for SIP to SIP trunk calls on Cisco Unified CME, allowing less consumption of resources on Cisco Unified CME.

The media flow around feature eliminates the need to terminate RTP and re-originate on Cisco Unified CME. This reduces media switching latency and increases the call handling capacity for a Cisco Unified CME SIP trunk.

Media flow around is supported in the following scenarios:

- Single Number Reach (SNR) Push—If an SNR call on a SIP trunk is pushed over to a mobile user over another SIP trunk, the resulting connection is a SIP-SIP trunk call connection. If both SIP trunks are configured for media flow around, the media is allowed to flow around Cisco Unified CME for the resulting call.

- Call Forward—If a SIP trunk call is forwarded over another SIP trunk and both the SIP trunks are configured for media flow around, media flows around Cisco Unified CME for the resulting SIP-SIP trunk call. Media flow around is supported for all types of call forwarding, such as call forward night-service, call forward all, call forward busy, and call forward no-answer.
- Call Transfer—If a SIP trunk call is transferred over another SIP trunk and both SIP trunks are configured for media flow around, media flows around Cisco Unified CME for the resulting SIP-SIP trunk call. Media flow around is supported on both SIP-line-initiated call transfer and SCCP-line-initiated call transfers. It is supported for all types of call transfers, such as blind transfer, consult transfer, and full consult transfer.

Media is forced to flow through on different types of call flows including the SIP to SIP trunk call with asymmetric flow mode configurations or symmetric flow through configuration. In asymmetric flow mode configurations, one SIP leg is configured in the media flow around mode and another SIP leg is configured in the media flow through mode. In such cases, media is forced to flow through Cisco Unified CME.

Media is forced to flow through Cisco Unified CME for the following types of call flows:

- Any calls involving a SIP endpoint, a SCCP endpoint, PSTN trunks (BRI/PRI/FXO), or FXO circuits.
- SIP to SIP trunk call with either asymmetric flow mode configurations or symmetric flow through configurations.
- SIP to SIP trunk call that requires transcoding services on Cisco Unified CME.
- SIP to SIP trunk calls that require DTMF interworking with RFC2833 on one side, and SIP-Notify on the other side.
- SNR pullback to SCCP— When an SNR call is pulled back from a mobile phone to the local SCCP SNR extension, the call is connected to the SCCP SNR extension. Media is required to flow through Cisco Unified CME because one of the calls is from a SCCP SNR extension, which is local to Cisco Unified CME.

In Cisco Unified CME 8.5, the media flow around feature is turned on or turned off using the **media** command in voice service voip, dial-peer voip, and voice class media configuration modes. The configuration specified under voice class media configuration mode takes precedence over the configuration in dial-peer configuration mode. If the media configuration is not specified under voice class media or dial-peer configuration mode, then the global configuration specified under voice service voip takes precedence. For more information, see Enable Media Flow Mode on SIP Trunks, on page 205.

Overlap Dialing Support for SIP and SCCP IP Phones

Cisco Unified CME 8.5 and later versions support overlap dialing on SCCP and SIP IP phones such as 7942, 7945, 7962, 7965, 7970, 7971, and 7975.

In earlier versions of Cisco Unified CME, overlap dialing was not supported over PRI/BRI trunks for calls originating from SCCP or SIP IP phones. Dialing was always converted into enbloc dialing based on the dial-peer configuration and the dial-peer mapping application. Once dialpeer matching took place, no further dialing was possible and no overlap digit were sent over ISDN trunk, even though overlap dialing was supported over ISDN trunks.

SCCP IP phones currently support overlap dialing, but digits are converted to enbloc digits when it reaches Cisco Unified CME. Overlap dialing is supported on SIP IP phones using the KeyPad Markup Language (KPML) method.

With overlap dialing support, the dialed digits from the SIP or SCCP IP phones are passed across to the PRI/BRI trunks as overlap digits and not as enbloc digits, enabling overlap dialing on the PRI/BRI trunks as well.

For information on how to configure SCCP and SIP IP phones for overlap dialing, see Configure Overlap Dialing on SCCP IP Phones, on page 190 and Configure Overlap Dialing on SIP Phones, on page 207.

Unsolicited Notify for Shared Line and Presence Events for Cisco Unified SIP IP Phones

Before Cisco Unified CME 9.0, a Cisco Unified SIP IP phone receives NOTIFY messages that convey shared line and presence events from the Cisco Unified CME only by subscribing to such events. To subscribe, the IP phone sends a SUBSCRIBE message to the Cisco Unified CME with the type of event for which it wants to be notified. The Cisco Unified CME sends a NOTIFY message to alert the subscribed IP phone or subscriber of event updates.

In Unsolicited Notify, the Cisco Unified CME acquires the required information from the router configuration to create the implicit subscription and adds subscribers without a subscription request from Cisco Unified SIP IP phones. The Cisco Unified CME sends out NOTIFY messages to the IP phones for shared line or presence updates.

In Cisco Unified CME 9.0 and later versions, the Unsolicited Notify mechanism reduces network traffic particularly during Cisco Unified SIP IP phone registration using the bulk registration method. Through this registration method, the preferred notification method of the IP phone is embedded in the registration message.

Note Configuring TCP as the transport layer protocol under voice register pool configuration mode enables bulk registration with negotiation for the Unsolicited Notify mechanism.

The Unsolicited Notify mechanism supports backward compatibility with all existing Cisco Unified SIP IP phone features. This mechanism is also the defacto notify mechanism in newer IP phone and Cisco Unified CME features, such as SNR Mobility.

From the end-user perspective, the following are the only two discernible differences between the SUBSCRIBE/NOTIFY and the Unsolicited Notify mechanisms:

- **show presence subscription** and **show shared-line** commands display different subscription IDs for each mechanism.
- With the SUBSCRIBE/NOTIFY mechanism, a Cisco Unified SIP IP phone needs to refresh the Cisco Unified CME subscription. In Unsolicited Notify mode, the subscription is permanent and does not need a refresh as long as the IP phone remains registered.

Restriction

- Because Unsolicited Notify is negotiated during bulk registration, the mechanism is not available on Cisco Unified SIP IP phones that do not have bulk registration turned on or have firmware that do not support bulk registration.
- Cisco Unified CME cannot disable the Unsolicited Notify mechanism. The system complies with and cannot override the requests of Cisco Unified SIP IP phones.
- In the absence of Cisco Unified SIP IP phone subscription information to distinguish if a notification event is for line or device monitoring, local device monitoring is not supported in the Unsolicited Notify mode.

Interface Support for Unified CME and Unified SRST

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

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

- Gigabit Ethernet Interface (IEEE 802.3z) (**interface gigabitethernet**)
- Loopback Interface (**interface loopback**)
- Fast Ethernet Interface (**interface fastethernet**)

The remaining Cisco IOS interfaces are not validated on Unified CME and Unified SRST. Hence, Unified CME and Unified SRST do not claim support for these interfaces. For more information on the Cisco IOS Interface commands, see Cisco IOS Interface and Hardware Component Command Reference.

For physical interfaces such as **interface gigabitethernet** and **interface fastethernet**, subinterfaces are supported. In a subinterface, virtual interfaces are created by dividing a physical interface into multiple logical interfaces. For Cisco routers, a subinterface uses the parent physical interface for sending and receiving data. Virtual interfaces (For example, **interface loopback**) do not support subinterfaces.

A subinterface for **interface gigabitethernet** is configured as follows:

```
Router(config)#interface gigabitEthernet 0/0.1
Router(config-subif)#exit
Router(config)#exit
```

Configure System-Level Parameters

Configure IP Phones in IPv4, IPv6, or Dual Stack Mode

Restriction

- Legacy IP phones are not supported.
- Multicast MOH and multicast paging features are not supported on IPv6 only phones. If you want to receive paging calls on IPv6 enabled phones, use the default multicast paging.
- Primary and secondary CME need to be provisioned with the same network type.
- MWI relay server must be in IPv4 network.
- Presence server must be IPv4 only.
- Video endpoints, such as CUVA and 7985, are not supported in IPv6
- TAPI client is not supported in IPv6.
- All HTTP based IPv6 services are not supported.
- IOS TFTP server is not supported in IPv6.
- If protocol mode is IPv4, you can only configure IPv4 as the source IP-address, if protocol mode is IPv6 you can only configure IPv6 as the source IP address and if the protocol mode is dual-stack, you can configure both IPv4 and IPv6 source addresses.

Before You Begin

- Cisco Unified CME 8.0 or later version.
- IPv6 CEF must be enabled for dual-stack configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **protocol mode** {**ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**protocol mode** {**ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]} **Example:** `Router(config-telephony)# protocol mode dual-stack preference ipv6`	Allows SCCP phones to interact with phones on IPv6 voice gateways. You can configure phones for IPv4 addresses, IPv6 address es, or for a dual-stack mode • **ipv4—**Allows you to set the protocol mode as an IPv4 address. • **ipv6—**Allows you to set the protocol mode as an IPv6 address. • **dual-stack—**Allows you to set the protocol mode for both IPv4 and IPv6 addresses. • **preference—**Allows you to choose a preferred IP address family if protocol mode is dual-stack.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Example

```
telephony-service
protocol mode dual-stack preference ipv6
....
ip source-address 10.10.2.1 port 2000
ip source-address 2000:A0A:201:0:F:35FF:FF2C:697D
```

Configure IPv6 Source Address for SCCP IP Phones

Restriction

- IPv6 option only appears if protocol mode is in dual-stack or IPv6.
- Do not change the default port number (2000) in the **ip source-address** configuration command. If you change the port number, IPv6 CEF packet switching engine may not be able to handle the IPv6 SCCP phones and various packet handling problems may occur.

Before You Begin

Cisco Unified CME 8.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **ip source-address** {*ipv4 address* | *ipv6 address*} **port** *port* [**secondary** {*ipv4 address* | *ipv6 address* } [**rehome** *seconds*]] [**strict-match**]
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters the telephony-service configuration mode.
Step 4	**ip source-address** {*ipv4 address* | *ipv6 address*} **port** *port* [**secondary** {*ipv4 address* | *ipv6 address* } [**rehome** *seconds*]] [**strict-match**] **Example:** `Router(config-telephony)# ip source-address 10.10.10.33 port`	Allows to configure an IPv4 or IPv6 address as an IP source-address for phones to communicate with a Cisco Unified CME router. • *ipv4 address*—Allows phones to communicate with phones or voice gateways in an IPv4 network. *ipv4 address* can only be configured with an IPv4 address or a dual-stack mode.

	Command or Action	Purpose
	`2000 ip source-address 2001:10:10:10::`	• *ipv6 address*—Allows phones to communicate with phones or voice gateways in an IPv6 network. *ipv6 address* can only be configured with an IPv6 address or a dual-stack mode. • (Optional) **port** *port*—TCP/IP port number to use for SCCP. Range is from 2000 to 9999. Default is 2000. For dual-stack, port is only configured with an IPv4 address. • (Optional) **secondary**—Cisco Unified CME router with which phones can register if the primary Cisco Unified CME router fails. • (Optional) **rehome** *seconds*—Used only by Cisco Unified IP phones that have registered with a Cisco Unified Survivable Remote Site Telephony (SRST) router. This keyword defines a delay that is used by phones to verify the stability of their primary SCCP controller (Cisco Unified Communication Manager or Cisco Unified CME) before the phones re-register with it. This parameter is ignored by phones unless they are registered to a secondary Cisco Unified SRST router. The range is from 0 to 65535 seconds. The default is 120 seconds. The use of this parameter is a phone behavior and is subject to change, based on the phone type and phone firmware version. • (Optional) **strict-match**— Requires strict IP address checking for registration.
Step 5	**end** **Example:** `outer(config-telephony)# end`	Returns to privileged EXEC mode.

Verify IPv6 and Dual-Stack Configuration

Step 1 The following example shows a list of success messages that are printed during Cisco IOS boot up. These messages confirm whether IPv6 has been enabled on interfaces (for example, EDSP0.1 to EDSP0.5) specific to exchanging RTP packets with SCCP endpoints.

Example:

```
Router#
00:00:33: %EDSP-6-IPV6_ENABLED: IPv6 on interface EDSP0 added.
00:00:34: %EDSP-6-IPV6_ENABLED: IPv6 on interface EDSP0.1 added.
00:00:34: %EDSP-6-IPV6_ENABLED: IPv6 on interface EDSP0.2 added.
00:00:34: %EDSP-6-IPV6_ENABLED: IPv6 on interface EDSP0.3 added.
00:00:34: %EDSP-6-IPV6_ENABLED: IPv6 on interface EDSP0.4 added.
00:00:34: %EDSP-6-IPV6_ENABLED: IPv6 on interface EDSP0.5 added.
00:00:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
00:00:34: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
```

```
00:00:34: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.2, changed state to up
.
```

Step 2 Use the **show ephone socket** command to verify if IPv4 only, IPv6 only, or dual-stack (IPv4/IPv6) is configured in Cisco Unified CME. In the following example, SCCP TCP listening socket (skinny_tcp_listen_socket fd) values 0 and 1 verify dual-stack configuration. When IPv6 only is configured, the **show ephone socket** command displays SCCP TCP listening socket values as (-1) and (0). The listening socket is closed if the value is (-1). When IPv4 only is configured, the **show ephone socket** command displays SCCP TCP listening socket values as (0) and (-1).

Example:

```
Router# show ephone socket
skinny_tcp_listen_socket fd = 0

skinny_tcp_listen_socket (ipv6) fd = 1


skinny_secure_tcp_listen_socket fd = -1

skinny_secure_tcp_listen_socket (ipv6) fd = -1


Phone 7,

skinny_sockets[15] fd = 16 [ipv6]

read_buffer 0x483C0BC4, read_offset 0, read_header N, read_length 0

resend_queue 0x47EC69EC, resend_offset 0, resend_flag N, resend_Q_depth 0

MTP 1,

skinny_sockets[16] fd = 17

read_buffer 0x483C1400, read_offset 0, read_header N, read_length 0

resend_queue 0x47EC6978, resend_offset 0, resend_flag N, resend_Q_depth 0

Phone 8,

skinny_sockets[17] fd = 18 [ipv6]

read_buffer 0x483C1C3C, read_offset 0, read_header N, read_length 0

resend_queue 0x47EC6904, resend_offset 0, resend_flag N, resend_Q_depth 0
```

Step 3 Use the show ephone summary command to verify the IPv6 or IPv4 addresses configured for ephones. The following example displays IPv6 and IPv4 addresses for different ephones:

Example:

```
Router# show ephone summary
ephone-2[1] Mac:0016.46E0.796A TCP socket:[7] activeLine:0 whisperLine:0 REGISTERED

mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
privacy:1 primary_dn: 1*

IPv6:2000:A0A:201:0:216:46FF:FEE0:796A* IP:10.10.10.12 7970 keepalive 599 music 0 1:1

sp1:2004


ephone-7[6] Mac:0013.19D1.F8A2 TCP socket:[6] activeLine:0 whisperLine:0 REGISTERED

mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0 reset_sent:0 debug:0
privacy:0 primary_dn: 13*
```

```
IP:10.10.10.14 * Telecaster 7940 keepalive 2817 music 0 1:13 2:28
```

Configure Bulk Registration

To configure bulk registration for registering a block of phone numbers with an external registrar so that calls can be routed to Cisco Unified CME from a SIP network, perform the following steps.

Numbers that match the number pattern defined by using the **bulk** command can register with the external registrar. The block of numbers that is registered can include any phone that is attached to Cisco Unified CME or any analog phone that is directly attached to an FXS port on a Cisco Unified CME router.

Note Use the **no reg** command to specify that an individual directory number should not register with the external registrar. For configuration information, see Disable SIP Proxy Registration for a Directory Number, on page 276.

Before You Begin

Cisco Unified CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode** *cme*
5. **bulk** *number*
6. **exit**
7. **sip-ua**
8. **registrar** {**dns**: *address* | **ipv4**: *destination-address*} **expires** *seconds* [**tcp**] [**secondary**] **no registrar** [**secondary**]
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**mode** *cme* **Example:** `Router(config-register-global)# mode cme`	Enables mode for provisioning SIP phones in Cisco Unified CME.
Step 5	**bulk** *number* **Example:** `Router(config-register-global)# bulk 408526....`	Sets bulk registration for E.164 numbers that will register with a SIP proxy server. • *number*—Unique sequence of up to 32 characters, including wild cards and patterns that represents E.164 numbers that will register with a SIP proxy server.
Step 6	**exit** **Example:** `Router(config-register-pool)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 7	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user agent (UA) configuration mode for configuring the user agent.
Step 8	**registrar** {**dns**: *address* | **ipv4**: *destination-address*} **expires** *seconds* [**tcp**] [**secondary**] **no registrar** [**secondary**] **Example:** `Router(config-sip-ua)# registrar server ipv4:1.5.49.240`	Enables SIP gateways to register E.164 numbers with a SIP proxy server.
Step 9	**end** **Example:** `Router(config-sip-ua)# end`	Exits SIP UA configuration mode and enters privileged EXEC mode.

Examples

The following example shows that all phone numbers that match the pattern “408555...” can register with a SIP proxy server (IP address 1.5.49.240):

```
voice register global
 mode cme
```

```
 bulk 408555….
sip-ua
 registrar ipv4:1.5.49.240
```

Configure Bulk Registration for SIP IP Phones

Before You Begin

- Cisco Unified CME 8.6 or a later version.
- Phone firmware 8.3 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *tag*
4. **session-transport** {**tcp** | **udp**}
5. **number** *tag* **dn** *tag*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool** *tag* **Example:** `Router(config)#voice register pool 20`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.
Step 4	**session-transport** {**tcp** | **udp**} **Example:** `Router(config-register-pool)#session-transport tcp`	Specifies the transport layer protocol that a SIP phone uses to connect to Cisco Unified CME. • **tcp**—TCP is used for bulk registration. • **udp**—UDP is used for line registration.
Step 5	**number** *tag* **dn** *tag* **Example:** `Router(config-register-pool)#number 1 dn 2`	Associates a directory number with the SIP phone being configured. • **dn** *dn-tag*—Identifies the directory number for this SIP phone as defined by the voice register **dn** command.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Verify Phone Registration Type and Status

You can verify phone registration type and status using the **show voice register pool** command. The following example shows that the Cisco Unified IP phone 7970 used the bulk registration method and completed the registration process:

```
Router#sh voice register pool 20
 Pool Tag 20
Config:
  Mac address is 001B.2A89.3698
  Type is 7970
  Number list 1 : DN 20
  Number list 2 : DN 2
  Number list 3 : DN 24
  Number list 4 : DN 4
  Number list 5 : DN 6
  Number list 6 : DN 7
  Number list 7 : DN 17
  Number list 8 : DN 23
  Proxy Ip address is 0.0.0.0
  Current Phone load version is Cisco-CP7970G/9.0.1
  DTMF Relay is enabled, rtp-nte, sip-notify
  Call Waiting is enabled
  DnD is disabled
  Video is disabled
  Camera is disabled
  Busy trigger per button value is 0
  speed-dial blf 1 6779 label 6779_device
  speed-dial blf 2 3555 label 3555_remote
  speed-dial blf 3 6130 label 6130
  speed-dial blf 4 3222 label 3222_remote_dev
  fastdial 1 1234
  keep-conference is enabled
  username johndoe password cisco
  template is 1
  kpml signal is enabled
  Lpcor Type is none
  Transport type is tcp
  service-control mechanism is supported
  Registration method: bulk - completed
  registration Call ID is 001b2a89-3698017e-68646967-126b902e@28.18.88.33

  Privacy is configured:  init status: ON, current status: ON
  Privacy button is enabled
  active primary line is: 6010
```

Set Up Cisco Unified CME for SCCP Phones

To identify filenames and the location of phone firmware for phone types to be connected, specify the port for phone registration, and specify the number of phones and directory numbers to be supported, perform the following steps.

Restriction DSCP requires Cisco Unified CME 7.1 or a later version. If DSCP is configured for the gateway interface using the **service-policy** command or for the dial peer using the ip qos dscp command, the value set with those commands takes precedence over the DSCP value configured in this procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tftp-server** *device***:***filename*
4. **telephony-service**
5. **load** *phone-type firmware-file*
6. **max-ephones** *max-phones*
7. **max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**]
8. **ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**]
9. **ip qos dscp** {{*number* | *af* | *cs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}}
10. **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	**tftp-server** *device***:***filename* **Example:** `Router(config)# tftp-server flash:P00307020300.bin`	(Optional) Creates TFTP bindings to permit IP phones served by the Cisco Unified CME router to access the specified file. • A separate **tftp-server** command is required for each phone type. • Required for Cisco Unified CME 7.0/4.3 and earlier versions. • Cisco Unified CME 7.0(1) and later versions: Required only if the location for cnf files is not flash or slot 0, such as system memory or a TFTP server url. Use the complete filename, including the file suffix, for phone firmware versions later than version 8.2(2) for all phone types.
Step 4	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 5	**load** *phone-type firmware-file* **Example:** `Router(config-telephony)# load 7960-7940 P00307020300`	Identifies a Cisco Unified IP phone firmware file to be used by phones of the specified type when they register. • A separate **load** command is required for each IP phone type. • firmware-file—Filename is case-sensitive. ◦ Cisco Unified CME 7.0/4.3 and earlier versions: Do not use the .sbin or .loads file extension except for the Cisco ATA and Cisco Unified IP Phone 7905 and 7912. ◦ Cisco Unified CME 7.0(1) and later versions: Use the complete filename, including the file suffix, for phone firmware versions later than version 8.2(2) for all phone types. **Note** If you are loading a firmware file larger than 384 KB, you must first load a file for that phone type that is smaller than 384 KB and then load the larger file.
Step 6	**max-ephones** *max-phones* **Example:** `Router(config-telephony)# max-ephones 24`	Sets the maximum number of phones that can register to Cisco Unified CME. • Maximum number is platform and version-specific. Type **?** for range. • In Cisco Unified CME 7.0/4.3 and later versions, the maximum number of phones that can register is different from the maximum number of phones that can be configured. The maximum number of phones that can be configured is 1000. • In versions earlier than Cisco Unified CME 7.0/4.3, this command restricted the number of phones that could be configured on the router.
Step 7	**max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**] **Example:** `Router(config-telephony)# max-dn 200 no-reg primary`	Limits number of directory numbers to be supported by this router. • Maximum number is platform and version-specific. Type **?** for value.
Step 8	**ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**] **Example:** `Router(config-telephony)# ip source-address 10.16.32.144`	Identifies the IP address and port number that the Cisco Unified CME router uses for IP phone registration. • **port** *port*—(Optional) TCP/IP port number to use for SCCP. Range is 2000 to 9999. Default is 2000. • **any-match**—(Optional) Disables strict IP address checking for registration. This is the default. • **strict-match**—(Optional) Instructs the router to reject IP phone registration attempts if the IP server address used by the phone does not exactly match the source address.

	Command or Action	Purpose
Step 9	**ip qos dscp** {{*number* | *af* | *cs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}} **Example:** `Router(config-telephony)# ip qos dscp af43 video`	Sets the DSCP priority levels for different types of traffic.
Step 10	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Examples

The following example shows different DSCP settings for media, signaling, video, and services enabled with the ip qos dscp command:

```
telephony-service
load 7960-7940 P00308000500
max-ephones 100
max-dn 240
ip source-address 10.10.10.1 port 2000
ip qos dscp af11 media
ip qos dscp cs2 signal
ip qos dscp af43 video
ip qos dscp 25 service
cnf-file location flash:
.
.
```

Set Date and Time Parameters for SCCP Phones

To specify the format of the date and time that appears on all SCCP phones in Cisco Unified CME, perform the following steps.

Note For certain phones, such as the Cisco Unified IP Phones 7906, 7911, 7931, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, and 7975, you must configure the **time-zone** command to ensure that the correct time stamp appears on the phone display. This command is not required for Cisco Unified IP Phone 7902G, 7905G, 7912G, 7920, 7921, 7935, 7936, 7940, 7960, or 7985G.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **date-format** {**dd-mm-yy** | **mm-dd-yy** |**yy-dd-mm** | **yy-mm-dd**}
5. **time-format** {**12** | **24**}
6. **time-zone** *number*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**date-format** {**dd-mm-yy** | **mm-dd-yy** |**yy-dd-mm** | **yy-mm-dd**} **Example:** `Router(config-telephony)# date-format yy-mm-dd`	(Optional) Sets the date format for phone display. • Default: **mm-dd-yy**.
Step 5	**time-format** {**12** | **24**} **Example:** `Router(config-telephony)# time-format 24`	(Optional) Selects a 12-hour or 24-hour clock for the time display format on phone display. • Default: **12**.
Step 6	**time-zone** *number* **Example:** `Router(config-telephony)# time-zone 2`	Sets time zone for SCCP phones. • Not required for Cisco Unified IP Phone 7902G, 7905G, 7912G, 7920, 7921, 7935, 7936, 7940, 7960, or 7985G. • Default: 5, Pacific Standard/Daylight Time (-480).
Step 7	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Block Automatic Registration for SCCP Phones

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **no auto-reg-ephone**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**no auto-reg-ephone** **Example:** `Router(config-telephony)# no auto-reg-ephone`	Disables automatic registration of Cisco Unified IP phones that are running SCCP but are not explicitly configured in Cisco Unified CME. • Default: Enabled.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Define Per-Phone Configuration Files and Alternate Location for SCCP Phones

Restriction

- TFTP does not support file deletion. When configuration files are updated, they overwrite any existing configuration files with the same name. If you change the configuration file location, files are not deleted from the TFTP server.
- Generating configuration files on flash memory or slot 0 memory can take up to a minute, depending on the number of files being generated.
- For smaller routers such as the Cisco 2600 series routers, you must manually enter the **squeeze** command to erase files after changing the configuration file location or entering any commands that trigger the deletion of configuration files. Unless you use the **squeeze** command, the space used by the moved or deleted configuration files is not usable by other files.
- If VRF Support on Cisco Unified CME is configured and the **cnf-file location** command is configured for system:, the per phone or per phone type file for an ephone in a VRF group is created in *system:/its/vrf<group-tag>/*. The vrf directory is automatically created and appended to the TFTP path. No action is required on your part. Locale files are still created in system:/its/.
- If VRF Support on Cisco Unified CME is configured and the **cnf-file location** command is configured as **flash:** or **slot0:**, the per phone or per phone type file for an ephone in a VRF group is named *flash:/its/vrf<group-tag>_<filename> or slot0:/its/vrf<group-tag>_filename>*. The vrf directory is automatically created and appended to the TFTP path. No action is required on your part. The location of the locale files is not changed.

To define a location other than system:/its for storing configuration files for per-phone and per-phone type configuration files, perform the following steps.

Before You Begin

- Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **cnf-file location** {**flash:** | **slot0:** | **tftp** *tftp-url*}
5. **cnf-file** {**perphonetype** | **perphone**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**cnf-file location** {**flash:** | **slot0:** | **tftp** *tftp-url*} **Example:** `Router(config-telephony)# cnf-file location flash:`	Specifies a location other than system:/its for storing phone configuration files. • Required for per-phone or per-phone type configuration files.
Step 5	**cnf-file** {**perphonetype** | **perphone**} **Example:** `Router(config-telephony)# cnf-file perphone`	Specifies whether to use a separate file for each type of phone or for each individual phone. • Required if you configured the **cnf-file location** command.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

The following example selects flash memory as the configuration file storage location and per-phone as the type of configuration files that the system generates:

```
telephony-service
 cnf-file location flash:
 cnf-file perphone
```

What to Do Next

If you changed the configuration file storage location, use the **option 150 ip** command to update the address. See Change the TFTP Address on a DHCP Server, on page 144.

Modify Defaults for Timeouts for SCCP Phones

To configure values for system-level intervals for which default values are typically adequate, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **timeouts busy** *seconds*
5. **timeouts interdigit** *seconds*
6. **timeouts ringing** *seconds*
7. **keepalive** *seconds*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**timeouts busy** *seconds* **Example:** `Router(config-telephony)# timeouts busy 20`	(Optional) Sets the length of time after which calls that are transferred to busy destinations are disconnected. • *seconds*—Number of seconds. Range is 0 to 30. Default is 10.
Step 5	**timeouts interdigit** *seconds* **Example:** `Router(config-telephony)# timeouts interdigit 30`	(Optional) Configures the interdigit timeout value for all Cisco Unified IP phones attached to the router. • *seconds*—Number of seconds before the interdigit timer expires. Range is 2 to 120. Default is 10.
Step 6	**timeouts ringing** *seconds* **Example:** `Router(config-telephony)# timeouts ringing 30`	(Optional) Sets the duration, in seconds, for which the Cisco Unified CME system allows ringing to continue if a call is not answered. Range is 5 to 60000. Default is 180.
Step 7	**keepalive** *seconds* **Example:** `Router(config-telephony)# keepalive 45`	(Optional) Sets the time interval, in seconds, between keepalive messages that are sent to the router by Cisco Unified IP phones.

	Command or Action	Purpose
		• The default is usually adequate. If the interval is set too large, it is possible for notification to be delayed when a system goes down. • Range: 10 to 65535. Default: 0.
Step 8	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Redundant Router for SCCP Phones

Before You Begin

- Cisco Unified CME 4.0 or a later version.
- The secondary router's running configuration must be identical to that of the primary router.
- The physical configuration of the secondary router must be as described in Redundant Cisco Unified CME Router for SCCP Phones, on page 160.
- Phones that use this feature must be configured with the **type** command, which guarantees that the appropriate phone configuration file will be present.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **ip source-address** *ip-address* [**port** *port*] [**secondary** *ip-address* [**rehome** *seconds*]] [**any-match** | **strict-match**]
5. **exit**
6. **voice-port** *slot-number* / *port*
7. **signal ground-start**
8. **incoming alerting ring-only**
9. **ring number** *number*
10. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**ip source-address** *ip-address* [**port** *port*] [**secondary** *ip-address* [**rehome** *seconds*]] [**any-match** | **strict-match**] **Example:** `Router(config-telephony)# ip source-address 10.0.0.1 port 2000 secondary 10.2.2.25`	Identifies the IP address and port number that the primary Unified CME router uses for IP phone registration. • *ip-address*—Address of the primary Unified CME router. • **port** *port*—(Optional) TCP/IP port number to use for SCCP. Range is 2000 to 9999. Default is 2000. • **secondary** *ip-address*—Indicates a backup Unified CME router. • **rehome** *seconds*—Not used by Unified CME. Used only by phones registered to Cisco Unified SRST. • **any-match**—(Optional) Disables strict IP address checking for registration. This is the default. • **strict-match**—(Optional) Router rejects IP phone registration attempts if the IP server address used by the phone does not exactly match the source address.
Step 5	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 6	**voice-port** *slot-number* / *port* **Example:** `Router(config)# voice-port 2/0`	Enters voice-port configuration mode for the FXO voice port for DID calls from the PSTN.
Step 7	**signal ground-start** **Example:** `Router(config-voiceport)# signal ground-start`	Specifies ground-start signaling for a voice port.

	Command or Action	Purpose
Step 8	**incoming alerting ring-only** **Example:** `Router(config-voiceport)# incoming alerting ring-only`	Instructs the FXO ground-start voice port to detect incoming calls by detecting incoming ring signals.
Step 9	**ring number** *number* **Example:** `Router(config-voiceport)# ring number 3`	(Required only for the secondary router) Sets the maximum number of rings to be detected before answering an incoming call over an FXO voice port. • *number*—Number of rings detected before answering the call. Range is 1 to 10. Default is 1. **Note** For an incoming FXO voice port on a secondary Cisco Unified CME router, set this value higher than is set on the primary router. We recommend setting this value to 3 on the secondary router.
Step 10	**end** **Example:** `Router(config-voiceport)# end`	Returns to privileged EXEC mode.

Configure Redundant Router for SIP Phones

Before You Begin

- Cisco Unified CME 11.6 or a later version.
- Auto-register configuration is recommended only on the primary router.
- XML interface for secondary backup router is configured. See Configure the XML Interface for the Secondary Backup Router, on page 189.

Note It is recommended to configure the XML interface for a seamless failover from primary to secondary Cisco Unified CME. Else, there is delay in the phones getting registered to secondary Cisco Unified CME due to mismatch in the configuration version timestamp.

- Ensure that you configure version stamp synchronization on the primary router. See Configure Version Stamp Synchronization on the Primary Router, on page 188.

Note It is recommended to configure version stamp synchronization for a seamless failover from primary to secondary Cisco Unified CME. Else, there is delay in the phones getting registered to secondary Cisco Unified CME.

Restriction

- Active calls are not supported when switchover happens from primary router to the secondary router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **source-address** *ip-address* [**port** *port*] [**secondary** *ip-address*]
5. **keepalive** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 4	**source-address** *ip-address* [**port** *port*] [**secondary** *ip-address*] **Example:** `Router(config-register-global)# source-address 10.6.21.4 port 6000 secondary 10.6.50.6`	Identifies the IP address and port number that the Cisco Unified CME router uses for IP phone registration. • *ip-address*—Address of the primary Cisco Unified CME router. • **port** *port*—(Optional) TCP/IP port number to use for SIP. Range is 2000 to 9999. Default is 5060 for SIP. • **secondary** *ip-address*—Indicates a backup Cisco Unified CME router.
Step 5	**keepalive** *seconds* **Example:** `Router(config-register-global)# keepalive 200`	Sets the length of the time interval between successive keepalive messages from the SIP phones to Cisco Unified CME router. Default is 120 seconds.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-register-global)# end`	Returns to privileged EXEC mode.

Configure Version Stamp Synchronization on the Primary Router

To configure the primary router to enable automatic synchronization of 'version stamp' with secondary backup router, perform the following steps.

Tip All phone-related configurations are tagged with a 'version stamp' that indicates when the last configuration change was made.

Before You Begin

- XML interface for secondary backup router is configured. See Configure the XML Interface for the Secondary Backup Router, on page 189.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **standby username** *username* **password** *password*
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.

	Command or Action	Purpose
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony service configuration mode.
Step 4	**standby username** *username* **password** *password* **Example:** `Router(config-telephony)# standby username user23 password 3Rs92uzQ`	Defines an authorized user. • Same username and password that is defined in Configure the XML Interface for the Secondary Backup Router, on page 189.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure the XML Interface for the Secondary Backup Router

To configure the secondary backup router to activate the XML interface required to receive "version stamp" configuration change information from the primary router, perform the following steps.

Restriction

- Automatic synchronization for new or replacement routers is not supported.

Before You Begin

- The XML interface, provided through the Cisco IOS XML Infrastructure (IXI), must be configured. See Configuring the XML API.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **xml user** *user-name* **password** *password privilege-level*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony service configuration mode.
Step 4	**xml user** *user-name* **password** *password* *privilege-level* **Example:** `Router(config-telephony)# xml user user23 password 3Rs92uzQ 15`	Defines an authorized user. • *user-name*—Username of the authorized user. • *password*—Password to use for access. • *privilege-level*—Level of access to Cisco IOS commands to be granted to this user. Only the commands with the same or a lower level can be executed via XML. Range is 0 to 15.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Overlap Dialing on SCCP IP Phones

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **overlap-signal**
5. **exit**
6. **ephone** *phone-tag*
7. **overlap-signal**
8. **exit**
9. **ephone-template** *template-tag*
10. **overlap-signal**
11. **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	**telephony-service** **Example:** `Router(config)telephony-service`	Enters telephony-service configuration mode.
Step 4	**overlap-signal** **Example:** `Router(config-telephony)#overlap-signal`	Allows to configure overlap signaling support for SCCP IP phones.
Step 5	**exit** **Example:** `Router(config-telephony)#exit`	Exits telephony-service configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)ephone 10`	Enters ephone configuration mode.
Step 7	**overlap-signal** **Example:** `Router(config-ephone)overlap-signal`	Applies overlap signaling support for ephone.
Step 8	**exit** **Example:** `Router(config-ephone)exit`	Exits ephone configuration mode.
Step 9	**ephone-template** *template-tag* **Example:** `Router(config)ephone-template 10`	Enters ephone-template configuration mode.
Step 10	**overlap-signal** **Example:** `Router(config-ephone-template)#overlap-signal`	Applies overlap signaling support to ephone template.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(config-ephone-template)# end`	Returns to privileged EXEC mode.

Set Up Cisco Unified CME for SIP Phones

To identify filenames and location of phone firmware for phone types to be connected, to specify the port for phone registration, and to specify the number of phones and directory numbers to be supported, perform the following steps.

Note If your Cisco Unified CME system supports SCCP and SIP phones, do not connect your SIP phones to your network until after you have verified the configuration profile for the SIP phone.

Restriction

- SIP endpoints are not supported on H.323 trunks. SIP endpoints are supported on SIP trunks only.
- Certain Cisco Unified IP phones, such as the Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE, are supported only in Cisco Unified CME 4.1 and later versions.
- DSCP requires Cisco Unified CME 7.1 or a later version. If DSCP is configured for the gateway interface using the **service-policy** command or for the dial peer using the **ip qos dscp** command, the value set with those commands takes precedence over the DSCP value configured in this procedure.

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode cme**
5. **source-address** *ip-address* [**port** *port*]
6. **load** *phone-type firmware-file*
7. **tftp-path** {**flash**: | **slot0:** | **tftp:**//*url*}
8. **max-pool** *max-phones*
9. **max-dn** *max-directory-numbers*
10. **authenticate** [**all**][**realm** *string*]
11. **ip qos dscp** {{*number* | *af* | *cs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}}
12. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**mode cme** **Example:** `Router(config-register-global)# mode cme`	Enables mode for provisioning SIP phones in Cisco Unified CME.
Step 5	**source-address** *ip-address* [**port** *port*] **Example:** `Router(config-register-global)# source-address 10.6.21.4`	Enables the Cisco Unified CME router to receive messages from SIP phones through the specified IP address and port. • **port** *port*—(Optional) TCP/IP port number. Range: 2000 to 9999. Default: 2000.
Step 6	**load** *phone-type firmware-file* **Example:** `Router(config-register-global)# load 7960-7940 P0S3-07-3-00`	Associates a phone type with a phone firmware file. • A separate load command is required for each phone type.

	Command or Action	Purpose
Step 7	**tftp-path** {**flash**: | **slot0:** | **tftp:**//*url*} **Example:** `Router(config-register-global)# tftp-path http://mycompany.com/files`	(Optional) Defines a location, other than system memory, from which the SIP phones will download configuration profile files. • Default: system memory (system:/cme/sipphone/).
Step 8	**max-pool** *max-phones* **Example:** `Router(config-register-global)# max-pool 10`	Sets maximum number of SIP phones to be supported by the Cisco Unified CME router. • Version- and platform-dependent; type ? for range. • In Cisco CME 3.4 to Cisco Unified CME 7.0: Default is maximum number supported by platform. • In Cisco Unified CME 7.0(1) and later versions: Default is 0.
Step 9	**max-dn** *max-directory-numbers* **Example:** `Router(config-register-global)# max-dn 20`	(Optional) Sets maximum number of directory numbers for SIP phones to be supported by the Cisco Unified CME router. • Required for Cisco Unified CME 7.0(1) and later versions. • In Cisco Unified CME 7.0(1) and later versions: Default is 0. Range is 1 to maximum number supported by platform. Type **?** for range. • In Cisco CME 3.4 to Cisco Unified CME 7.0: Default is 150 or maximum allowed on platform. Type ? for value.
Step 10	**authenticate** [**all**][**realm** *string*] **Example:** `Router(config-register-global)# authenticate all realm company.com`	(Optional) Enables authentication for registration requests in which the MAC address of the SIP phone cannot be identified by using other methods.
Step 11	**ip qos dscp** {{*number* | *af* | *cs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}} **Example:** `Router(config-register-global)# ip qos dscp af43 video`	Sets the DSCP priority levels for different types of traffic.
Step 12	**end** **Example:** `Router(config-register-global)# end`	Exits voice register global configuration mode and enters privileged EXEC mode.

Set Up Cisco Unified CME for SIP Phones

To identify filenames and location of phone firmware for phone types to be connected, to specify the port for phone registration, and to specify the number of phones and directory numbers to be supported, perform the following steps.

Note If your Cisco Unified CME system supports SCCP and SIP phones, do not connect your SIP phones to your network until after you have verified the configuration profile for the SIP phone.

Restriction

- SIP endpoints are not supported on H.323 trunks. SIP endpoints are supported on SIP trunks only.
- Certain Cisco Unified IP phones, such as the Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE, are supported only in Cisco Unified CME 4.1 and later versions.
- DSCP requires Cisco Unified CME 7.1 or a later version. If DSCP is configured for the gateway interface using the **service-policy** command or for the dial peer using the **ip qos dscp** command, the value set with those commands takes precedence over the DSCP value configured in this procedure.

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode cme**
5. **source-address** *ip-address* [**port** *port*]
6. **load** *phone-type firmware-file*
7. **tftp-path** {**flash**: | **slot0:** | **tftp:**//*url*}
8. **max-pool** *max-phones*
9. **max-dn** *max-directory-numbers*
10. **authenticate** [**all**][**realm** *string*]
11. **ip qos dscp** {{*number* | *af* | *cs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}}
12. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**mode cme** **Example:** `Router(config-register-global)# mode cme`	Enables mode for provisioning SIP phones in Cisco Unified CME.
Step 5	**source-address** *ip-address* [**port** *port*] **Example:** `Router(config-register-global)# source-address 10.6.21.4`	Enables the Cisco Unified CME router to receive messages from SIP phones through the specified IP address and port. • **port** *port*—(Optional) TCP/IP port number. Range: 2000 to 9999. Default: 2000.
Step 6	**load** *phone-type firmware-file* **Example:** `Router(config-register-global)# load 7960-7940 P0S3-07-3-00`	Associates a phone type with a phone firmware file. • A separate load command is required for each phone type.
Step 7	**tftp-path** {**flash**: | **slot0:** | **tftp://***url*} **Example:** `Router(config-register-global)# tftp-path http://mycompany.com/files`	(Optional) Defines a location, other than system memory, from which the SIP phones will download configuration profile files. • Default: system memory (system:/cme/sipphone/).
Step 8	**max-pool** *max-phones* **Example:** `Router(config-register-global)# max-pool 10`	Sets maximum number of SIP phones to be supported by the Cisco Unified CME router. • Version- and platform-dependent; type ? for range. • In Cisco CME 3.4 to Cisco Unified CME 7.0: Default is maximum number supported by platform. • In Cisco Unified CME 7.0(1) and later versions: Default is 0.

	Command or Action	Purpose
Step 9	**max-dn** *max-directory-numbers* **Example:** `Router(config-register-global)# max-dn 20`	(Optional) Sets maximum number of directory numbers for SIP phones to be supported by the Cisco Unified CME router. • Required for Cisco Unified CME 7.0(1) and later versions. • In Cisco Unified CME 7.0(1) and later versions: Default is 0. Range is 1 to maximum number supported by platform. Type **?** for range. • In Cisco CME 3.4 to Cisco Unified CME 7.0: Default is 150 or maximum allowed on platform. Type ? for value.
Step 10	**authenticate** [**all**][**realm** *string*] **Example:** `Router(config-register-global)# authenticate all realm company.com`	(Optional) Enables authentication for registration requests in which the MAC address of the SIP phone cannot be identified by using other methods.
Step 11	**ip qos dscp** {{*number* | *af* | *cs* | **default** | **ef**} {**media** | **service** | **signaling** | **video**}} **Example:** `Router(config-register-global)# ip qos dscp af43 video`	Sets the DSCP priority levels for different types of traffic.
Step 12	**end** **Example:** `Router(config-register-global)# end`	Exits voice register global configuration mode and enters privileged EXEC mode.

Set Date and Time Parameters for SIP Phones

Before You Begin

- Cisco CME 3.4 or a later version.
- **mode cme** command is enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **timezone** *number*
5. **date-format** [**d/m/y** | **m/d/y** | **y-d-m** |**y/d/m** | **y/m/d** | **yy-m-d**]
6. **time-format** {**12** | **24**}
7. **dst auto-adjust**
8. **dst** {**start** | **stop**} *month* [**day** day-of-month | **week** week-number | **day** day-of-week] **time** *hour:minutes*
9. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**timezone** *number* **Example:** `Router(config-register-global)# timezone 8`	Selects the time zone used for SIP phones in Cisco Unified CME. • Default: **5**, Pacific Standard/Daylight Time. Type **?** to display a list of time zones.
Step 5	**date-format** [**d/m/y** | **m/d/y** | **y-d-m** |**y/d/m** | **y/m/d** | **yy-m-d**] **Example:** `Router(config-register-global)# date-format yy-m-d`	(Optional) Selects the date display format on SIP phones in Cisco Unified CME. • Default: **m/d/y**.
Step 6	**time-format** {**12** | **24**} **Example:** `Router(config-register-global)# time-format 24`	(Optional) Selects the time display format on SIP phones in Cisco Unified CME. • Default: **12**.

	Command or Action	Purpose
Step 7	**dst auto-adjust** **Example:** `Router(config-register-global)# dst auto-adjust`	(Optional) Enables automatic adjustment of Daylight Saving Time on SIP phones in Cisco Unified CME. • To modify start and stop times for daylight savings time, use the **dst** command.

Step 8	**dst** {**start** | **stop**} *month* [**day** day-of-month | **week** week-number | **day** day-of-week] **time** *hour:minutes*
	
	Example:
	`Router(config-register-global)# dst start jan day 1 time 00:00`
	`Router(config-register-global)# dst stop mar day 31 time 23:59`
		(Optional) Sets the time period for Daylight Saving Time on SIP phones in Cisco Unified CME.
		• Required if automatic adjustment of Daylight Saving Time is enabled by using the **dst auto-adjust** command.
		• Default is Start: First week of April, Sunday, 2:00 a.m. Stop: Last week of October, Sunday 2:00 a.m.

Step 9	**end** **Example:** `Router(config-register-global)# end`	Returns to privileged EXEC mode.

Set Network Time Protocol for SIP Phones

To enable Network Time Protocol (NTP) for certain phones, such as the Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE, connected to Cisco Unified CME running SIP, perform the following steps.

Before You Begin

- Cisco Unified CME 4.1 or a later version.
- The firmware load 8.2(1) or a later version is installed for SIP phones to download. For upgrade information, see Upgrade or Downgrade SIP Phone Firmware, on page 108.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **ntp-server** *ip-address* [**mode** {**anycast** | **directedbroadcast** | **multicast** | **unicast**}]
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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set global parameters for all supported SIP phones in a Cisco Unified CME environment.
Step 4	**ntp-server** *ip-address* [**mode** {**anycast** | **directedbroadcast** | **multicast** | **unicast**}] **Example:** `Router(config-register-global)# ntp-server 10.1.2.3`	Synchronizes clock on this router with the specified NTP server.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Returns to privileged EXEC mode.

Enable HFS Download Service for SIP Phones

Restriction

- Only Cisco Unified 8951, 9951, and 9971 SIP IP Phones are supported.
- No IPv6 support for the HFS download service.

Before You Begin

Cisco Unified CME 8.8 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http port** *number*
5. **voice register global**
6. **mode cme**
7. **load** *phone-type firmware-file*
8. **create profile**
9. **exit**
10. **telephony-service**
11. **hfs enable** [**port** *port-number*]
12. **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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the underlying IOS HTTP server of the HFS infrastructure.
Step 4	**ip http port** *number* **Example:** `Router(config)# ip http port 60`	(Optional) Specifies the port where the HTTP service is run.
Step 5	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set global parameters for all supported Cisco SIP IP phones in a Cisco Unified CME.
Step 6	**mode cme** **Example:** `Router(config-register-global)# mode cme`	Enables the mode for configuring SIP IP phones in a Cisco Unified CME system.

	Command or Action	Purpose
Step 7	**load** *phone-type firmware-file* **Example:** `Router(config-register-global)# load 3951 SIP51.9.2.1S`	Associates a type of SIP IP phone with a phone firmware file.
Step 8	**create profile** **Example:** `Router(config-register-global)# create profile`	Generates the configuration profile files required for SIP IP phones.
Step 9	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global configuration mode.
Step 10	**telephony-service** **Example:** `Router (config)# telephony-service`	Enters telephony-service configuration mode for configuring Cisco Unified CME.
Step 11	**hfs enable** [**port** *port-number*] **Example:** `Router(config-telephony)# hfs enable port 5678`	Enables the HFS download service on a specified port. • **port** *port-number*—(Optional) Specifies the port where the HFS download service is enabled. Range is from 1024 to 65535. Port 80 is the default port. Port 6970 is the custom port. **Note** If the entered custom HFS port clashes with the underlying IP HTTP port, an error message is displayed and the command is disallowed.
Step 12	**end** **Example:** `Router(config-telephonyl)# end`	Exits to privileged EXEC mode.

Troubleshooting HFS Download Service

The **debug cme-hfs** command can be used to troubleshoot an attempt to download Cisco Unified SIP IP phone configuration and firmware files using the HFS service.

Configure HFS Home Path for SIP Phone Firmware Files

To configure a home path where any requested Cisco Unified SIP IP Phone firmware file that has no explicit binding can be searched and fetched using the HFS download service, perform the following steps.

Restriction

- Only Cisco 8951, 9951, and 9971 SIP IP Phones are supported.
- No IPv6 support for the HFS download service.

Before You Begin

Cisco Unified CME 8.8 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http port** *number*
5. **telephony-service**
6. **hfs enable** [**port** *port-number*]
7. **hfs home-path** *path*
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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the underlying IOS HTTP server of the HFS infrastructure.
Step 4	**ip http port** *number* **Example:** `Router(config)# ip http port 1234`	Specifies the port where the HTTP service is run.
Step 5	**telephony-service** **Example:** `Router (config)# telephony-service`	Enters telephony-service configuration mode for configuring Cisco Unified CME.

	Command or Action	Purpose
Step 6	**hfs enable** [**port** *port-number*] **Example:** `Router(config-telephony)# hfs enable port 6970`	Enables the HFS download service on a specified port.
Step 7	**hfs home-path** *path* **Example:** `Router(config-telephony)# hfs home-path flash:/cme/loads/`	Sets a home path directory for Cisco Unified SIP IP phone firmware files that can be searched and fetched using the HFS download service. **Note** The administrator must store the phone firmware files at the location set as the home path directory.
Step 8	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

Change Session-Level Application for SIP Phones

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **application** *application-name*
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.

	Command or Action	Purpose
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**application** *application-name* **Example:** `Router(config-register-global)# application sipapp2`	(Optional) Changes the default application for all dial peers associated with the SIP phones in Cisco Unified CME to the specified application. **Note** This command can also be configured in voice register pool configuration mode. The value set in voice register pool configuration mode has priority over the value set in voice register global mode.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits voice register global configuration mode and enters privileged EXEC mode.

Enable Media Flow Mode on SIP Trunks

Restriction

- If any media service (like transcoding and conferencing) is needed for SIP to SIP trunk call, at least one of the SIP trunks must be placed in flow through mode.
- If media needs to flow through Cisco Unified CME for voicemail calls, the SIP trunk going towards the voicemail must be in flow through mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media** [**flow around** | **flow through**]
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **media** {[**flow-around** | **flow-through**] **forking**}
8. **exit**
9. **voice class media** tag
10. **media** {[**flow-around** | **flow-through**] **forking**}
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)#voice service voip`	Enters voice service voip configuration mode.
Step 4	**media** [**flow around** | **flow through**] **Example:** `Router(conf-voi-serv)#media flow-around`	Enables global media setting for VoIP calls. • **flow around—**Allows the media to flow around the gateway. • **flow through—**Allows the media to flow through the gateway.
Step 5	**exit** **Example:** `Router(config-voi-ser)#exit`	Exits voice service voip configuration mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)#dial-peer voice 222 voip`	Enters dial-peer configuration mode to define a VoIP dial peer for the voice-mail system. • *tag***—**Defines the dial peer being configured. Range is 1 to 1073741823.
Step 7	**media** {[**flow-around** | **flow-through**] **forking**} **Example:** `Router(config-dial-peer)#media flow-around`	Enables media settings for voice dial-peer. • **flow-around—**Allows the media to flow around the gateway. • **flow-through—**Allows the media to flow through the gateway. • **forking—**Enables media forking.
Step 8	**exit** **Example:** `Router(config-ephone)exit`	Exits voip dial-peer configuration mode.
Step 9	**voice class media** tag **Example:** `Router(config)#voice class media 10`	Enters voice class media configuration mode. • *tag***—** Defines the voice class media tag being configured. Range is from 1 to 10000.

	Command or Action	Purpose
Step 10	**media** {[**flow-around** | **flow-through**] **forking**} **Example:** `Router(config-class)#media flow-around`	Enables media settings for voice dial-peer. • **flow-around—**Allows the media to flow around the gateway. • **flow-through—**Allows the media to flow through the gateway. • **forking—**Enables media forking.
Step 11	**end** **Example:** `Router(config-class)# end`	Returns to privileged EXEC mode.

Configure Overlap Dialing on SIP Phones

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **overlap-signal**
5. **exit**
6. **voice register pool** *pool-tag*
7. **overlap-signal**
8. **exit**
9. **voice register template** *template tag*
10. **overlap-signal**
11. **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.

	Command or Action	Purpose
Step 3	**voice register global** **Example:** `Router(config)voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**overlap-signal** **Example:** `Router(config-register-pool)overlap-signal`	Allows to configure overlap signaling support for SIP IP phones.
Step 5	**exit** **Example:** `Router(config-register-pool)exit`	Exits voice register pool configuration mode.
Step 6	**voice register pool** *pool-tag* **Example:** `Router(config)voice register pool 10`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 7	**overlap-signal** **Example:** `Router(config-register-global)overlap-signal`	Enables overlap signaling support for voice register global.
Step 8	**exit** **Example:** `Router(config-register-global)exit`	Exits voice register-template configuration mode.
Step 9	**voice register template** *template tag* **Example:** `Router(config)voice register template 5`	Enters voice register-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.
Step 10	**overlap-signal** **Example:** `Router(config-register-temp) overlap-signal`	Applies overlap signaling support for voice register-template.
Step 11	**end** **Example:** `Router(config-register-temp)# end`	Returns to privileged EXEC mode.

Configuration Examples for System-Level Parameters

Example for Bulk Registration Support for SIP Phones

The following example shows TCP and UDP configured for various phones. Notice that in Bulk Registration (TCP), only the primary directory number is displayed, while in Line Registration (UDP), all directory numbers are displayed.

```
Router# show sip-ua status registrar
Line          destination      expires(sec)  contact
transport     call-id
              peer
============================================================
1001          21.1.1.138       112           21.1.1.138
TCP           239665429027943@21.1.1.138
              40015
1009          21.1.1.138       118           21.1.1.138
UDP           239671730027945@21.1.1.138
              40019
1010          21.1.1.138       118           21.1.1.138
UDP           239671745127945@21.1.1.138
              40021
```

Example for IPv6 Support on Cisco Unified CME

```
!
ip source-route
!
!ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.10.1 10.10.10.9
ip dhcp excluded-address 192.168.2.1
ipv6 unicast-routing
ipv6 cef
ntp server 223.255.254.254
multilink bundle-name authenticated
isdn switch-type primary-5ess
!
voice service voip

allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
fax protocol cisco
```

```
sip
registrar server expires max 1200 min 300
!
!
!
voice register dn  1
number 2016
allow watch
name SIP-7961GE
label SIP2016
!
voice register dn  2
number 2017
!
!
voice logout-profile 1
!
voice logout-profile 2
number 2001 type normal
speed-dial 1 2004 label "7960-1"

!
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.255.0
duplex auto
speed auto
ipv6 address 2000:A0A:201:0:F:35FF:FF2C:697D/64
ipv6 enable
interface GigabitEthernet0/1
ip address 40.10.30.1 255.255.255.0
shutdown
duplex auto
speed auto
ipv6 address 2000::1/64
ipv6 address 2000::2/64
ipv6 address 2000::A/64
ipv6 address 3000::1/64
ipv6 address 4000::1/64
ipv6 address 9000::1/64
ipv6 address F000::1/64
ipv6 enable
!
i!
!
!
ip http server
!
ipv6 route 2001:20:20:20::/64 2000:A0A:201:0:F:35FF:FF2C:5
ipv6 route 2001:50:50:50::/64 2000:A0A:201:0:F:35FF:FF2C:5
!
tftp-server flash:P00308000500.bin
tftp-server flash:P00308000500.loads
p-server flash:cvm70sccp.8-5-2FT1-18.sbn
!
!
voice-port 0/0/0:23
!
!
mgcp fax t38 ecm
!
sccp local GigabitEthernet0/0
sccp ccm 10.10.10.2 identifier 1 version 7.0

sccp ccm 2000:A0A:201:0:F:35FF:FF2C:697D identifier 2 version 7.0

sccp
!
!
gateway
```

```
timer receive-rtp 1200
!
sip-ua

protocol mode dual-stack preference ipv6
!
!
telephony-service
protocol mode dual-stack preference ipv6
sdspfarm conference mute-on 111 mute-off 222
sdspfarm units 2
sdspfarm transcode sessions 20
sdspfarm tag 1 xcoder
sdspfarm tag 2 conference
conference hardware
no auto-reg-ephone
em logout 0:0 0:0 0:0

max-ephones 52
max-dn 192
ip source-address 10.10.10.2 port 2000
ip source-address 2000:A0A:201:0:F:35FF:FF2C:697D
service phone settingsAccess 1
service phone spanTOPCPort 0
timeouts transfer-recall 15
system message MOTO-CME1
url directories http://10.10.10.2:80/localdirectory
cnf-file location flash:
cnf-file perphone
load 7914 S00103020003
load 7911 SCCP11.8-5-2FT1-18S
load 7970 SCCP70.8-5-2FT1-18S
time-zone 5
max-conferences 4 gain -6
call-forward pattern .T
web admin system name cisco password cisco
web admin customer name admin password admin
transfer-system full-consult
```

Example for System-Level Parameters

The following example shows the system-level configuration for a Cisco Unified CME that can support up to 500 directory numbers on 100 phones. It sets up TFTP file sharing for phone firmware files for Cisco Unified IP Phones 7905, 7912, 7914, 7920, 7940, and 7960 and it loads those files.

```
tftp-server flash:ATA030100SCCP040211A.zup
! ATA 186/188 firmware
tftp-server flash:CP7902080001SCCP051117A.sbin
! 7902 firmware
tftp-server flash:CP7905080001SCCP051117A.sbin
! 7905 firmware
tftp-server flash:CP7912080001SCCP051117A.sbin
! 7912 firmware
tftp-server flash:cmterm_7920.4.0-02-00.bin
! 7914 firmware
tftp-server flash:P00503010100.bin
! 7920 firmware
tftp-server flash:S00104000100.sbn
! 7935 firmware
tftp-server flash:cmterm_7936.3-3-5-0.bin
! 7936 firmware
tftp-server flash:P0030702T023.bin
tftp-server flash:P0030702T023.loads
tftp-server flash:P0030702T023.sb2
! 7960/40 firmware
!
telephony-service
 max-ephones 100
 max-dn 500
 load ata ATA030100SCCP040211A
 load 7902 CP7902080001SCCP051117A
 load 7905 CP7905080001SCCP051117A
 load 7912 CP7912080001SCCP051117A
 load 7914 S00104000100
 load 7920 cmterm_7920.4.0-02-00
 load 7935 P00503010100
 load 7936 cmterm_7936.3-3-5-0
 load 7960-7940 P0030702T023
 ip source-address 10.16.32.144 port 2000
 create cnf-files version-stamp Jan 01 2002 00:00:00
 transfer-system full-consult

Cisco Unified IP Phone 7911, 7941, 7941-GE, 7961, 7961-GE, 7970, and 7971 require multiple
 files to be shared using TFTP. The following configuration example adds support for these
 phones.

tftp-server flash:SCCP11.7-2-1-0S.loads
tftp-server flash:term11.default.loads
tftp-server flash:apps11.1-0-0-72.sbn
tftp-server flash:cnu11.3-0-0-81.sbn
tftp-server flash:cvm11.7-2-0-66.sbn
tftp-server flash:dsp11.1-0-0-73.sbn
tftp-server flash:jar11.7-2-0-66.sbn
! 7911 firmware
!
tftp-server flash:TERM41.7-0-3-0S.loads
tftp-server flash:TERM41.DEFAULT.loads
tftp-server flash:TERM61.DEFAULT.loads
tftp-server flash:CVM41.2-0-2-26.sbn
tftp-server flash:cnu41.2-7-6-26.sbn
tftp-server flash:Jar41.2-9-2-26.sbn
! 7941/41-GE, 7961/61-GE firmware
!
tftp-server flash:TERM70.7-0-1-0s.LOADS
tftp-server flash:TERM70.DEFAULT.loads
tftp-server flash:TERM71.DEFAULT.loads
tftp-server flash:CVM70.2-0-2-26.sbn
```

```
tftp-server flash:cnu70.2-7-6-26.sbn

tftp-server flash:Jar70.2-9-2-26.sbn
! 7970/71 firmware
!
telephony-service
 load 7911 SCCP11.7-2-1-0S
 load 7941 TERM41.7-0-3-0S
 load 7961 TERM41.7-0-3-0S
 load 7941GE TERM41.7-0-3-0S
 load 7961GE TERM41.7-0-3-0S
 load 7970 TERM70.7-0-1-0s
 load 7971 TERM70.7-0-1-0s
 create cnf-files version-stamp Jan 01 2002 00:00:00
.
.
.
```

Example for Blocking Automatic Registration

The following example shows how to disable automatic ephone registration, display a log of attempted registrations, and then clear the log:

```
Router(config)# telephony-service

Router(config-telephony)# no auto-reg-ephone

Router(config-telephony)# exit

Router(config)# exit

Router# show ephone attempted-registrations


Attempting Mac address:


Num Mac Address DateTime DeviceType

-----------------------------------------------------------------------------


1 C863.8475.5417 22:52:05 UTC Thu Apr 28 2005 SCCP Gateway (AN)

2 C863.8475.5408 22:52:05 UTC Thu Apr 28 2005 SCCP Gateway (AN)

.....

25 000D.28D7.7222 22:26:32 UTC Thu Apr 28 2005 Telecaster 7960

26 000D.BDB7.A9EA 22:25:59 UTC Thu Apr 28 2005 Telecaster 7960

...

47 C863.94A8.D40F 22:52:17 UTC Thu Apr 28 2005 SCCP Gateway (AN)

48 C863.94A8.D411 22:52:18 UTC Thu Apr 28 2005 SCCP Gateway (AN)


49 C863.94A8.D400 22:52:15 UTC Thu Apr 28 2005 SCCP Gateway (AN)


Router# clear telephony-service ephone-attempted-registrations
```

Example for Enabling the HFS Download Service for Cisco Unified SIP IP Phone

The following example shows how to enable the HFS download service:

```
Router(config)# ip http server
Router(config)# ip http port 1234
Router (config)# telephony-service
Router(config-telephony)# hfs enable port 65500
```

Example for Configuring an HFS Home Path for Cisco Unified SIP IP Phone Firmware Files

The following example shows how a new directory called phone-load can be created under the root directory of the flash memory and set as the hfs home-path:

```
cassini-c2801#mkdir flash:phone-loads
Create directory filename [phone-loads]?
Created dir flash:phone-loads
cassini-c2801#sh flash:
-#- --length-- -----date/time------ path
1     13932728 Mar 22 2007 15:57:38 +00:00 c2801-ipbase-mz.124-1c.bin
2     33510140 Sep 18 2010 01:21:56 +00:00 rootfs9951.9-0-3.sebn
3       143604 Sep 18 2010 01:22:20 +00:00 sboot9951.111909R1-9-0-3.sebn
4         1249 Sep 18 2010 01:22:40 +00:00 sip9951.9-0-3.loads
5        66996 Sep 18 2010 01:23:00 +00:00 skern9951.022809R2-9-0-3.sebn
6        10724 Sep 18 2010 00:59:48 +00:00 dkern9951.100609R2-9-0-3.sebn
7      1507064 Sep 18 2010 01:00:24 +00:00 kern9951.9-0-3.sebn
8            0 Jan 5 2011 02:03:46 +00:00 phone-loads
14819328 bytes available (49192960 bytes used)
cassini-c2801#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cassini-c2801(config)#tele
cassini-c2801(config)#telephony-service
cassini-c2801(config-telephony)#hfs hom
cassini-c2801(config-telephony)#hfs home-path flash:?
WORD
cassini-c2801(config-telephony)#hfs home-path flash:phone-loads
cassini-c2801(config-telephony)#
```

Example for Verifying the HFS File Bindings of Cisco Unified SIP IP Phone Configuration and Firmware Files

The following is a sample output from the **show voice register hfs** command:

```
Router(config)#show voice register hfs
Fetch Service Enabled = Y
   App enabled port = 6970
   Use default port = N
   Registered session-id = 19

Default home path = flash:/
   Ongoing fetches from home = 0

HTTP File Server Bindings
   No. of bindings = 11
   No. of url table entries = 9
```

No. of alias table entries = 9

Example for Redundant Router for SCCP Phones

The following example is configured on the primary Cisco Unified CME router. It establishes the router at 10.5.2.78 as a secondary router. The voice port 3/0/0 is the FXO port for incoming calls from the PSTN. It is set to use ground-start signaling and to detect incoming calls by counting incoming ring signals.

```
telephony-service
 ip source-address 10.0.0.1 port 2000 secondary 10.5.2.78

voice-port 3/0/0
 signal ground-start
 incoming alerting ring-only
```

The secondary Cisco Unified CME router is configured with the same commands, except that the ring number command is set to 3 instead of using the default of 1.

```
telephony-service
 ip source-address 10.0.0.1 port 2000 secondary 10.5.2.78

voice-port 3/0/0
 signal ground-start
 incoming alerting ring-only
 ring number 3
```

Example for Redundant Router for SIP Phones

The following example is configured on the primary Cisco Unified CME router. It establishes the router at 10.6.50.6 as a secondary router with keepalive value set to 200 seconds.

Note For the synchronization to happen, additional configurations are needed. These configurations such as IXI, HTTP, and telephony-service are provided in the output.

```
voice register global
 source-address 10.6.21.4 port 6000 secondary 10.6.50.6
 keepalive 200

ip http server

ixi transport http
 response size 8
 no shutdown
 request outstanding 2
 request timeout 30

ixi application cme
 no shutdown
 response timeout -1

telephony-service
 ip source-address 10.6.21.4 secondary 10.6.50.6
 standby user cisco password cisco123
```

The secondary Cisco Unified CME router is configured with the same commands:

```
voice register global
 source-address 10.6.21.4 port 6000 secondary 10.6.50.6
 keepalive 200

ip http server

ixi transport http
 response size 8
```

```
 no shutdown
 request outstanding 2
 request timeout 30

ixi application cme
 no shutdown
 response timeout -1

telephony-service
 ip source-address 10.6.50.6
 xml user cisco password cisco123 15
```

Example for Media Flow Around Mode for SIP Trunks

The following example shows media flow-around enabled in voice service voip, voice class media, and dial peer configuration modes:

```
Router# show running config

!

!

voice service voip

ip address trusted list

ipv4 20.20.20.1

media flow-around

allow-connections sip to sip

vpn-group 1

vpn-gateway 1 https://9.10.60.254/SSLVPNphone

vpn-trustpoint 1 trustpoint cme_cert root

vpn-hash-algorithm sha-1

vpn-profile 1

keepalive 50

auto-network-detect enable

host-id-check disable

vpn-profile 2

mtu 1300

authen-method both

password-persistent enable

host-id-check enable

vpn-profile 4

fail-connect-time 50

sip

!

voice class media 10

media flow-around
```

```
!
!
!
dspfarm profile 1 conference
codec g711ulaw
maximum sessions 2
associate application SCCP
!
dial-peer voice 222 voip
media flow-around
!
dial-peer voice 10 voip
media flow-around
!
dial-peer voice 101 voip
end
```

Example for Configuring Overlap Dialing for SCCP IP Phones

The following example shows the **overlap-signal** command configured in telephony-service configuration mode, ephone template 10, and ephone 10:

```
The following example shows the overlap-signal command configured in telephony-service
configuration mode, ephone template 10, and ephone 10:
Router# show running config
!
!
telephony-service
max-ephones 25
max-dn 15
load 7906 SCCP11.8-5-3S.loads
load 7911 SCCP11.8-5-3S.loads
load 7921 CP7921G-1.3.3.LOADS
load 7941 SCCP41.8-5-3S.loads
load 7942 SCCP42.8-5-3S.loads
load 7961 SCCP41.8-5-3S.loads
load 7962 SCCP42.8-5-3S.loads
max-conferences 12 gain -6
web admin system name cisco password cisco
```

```
transfer-system full-consult
create cnf-files version-stamp Jan 01 2002 00:00:00
overlap-signal
!
ephone-template 1
button-layout 1 line
button-layout 3-6 blf-speed-dial
!
ephone-template 9
feature-button 1 Endcall
feature-button 3 Mobility
!
!
ephone-template 10
feature-button 1 Park
feature-button 2 MeetMe
feature-button 3 CallBack
button-layout 1 line
button-layout 2-4 speed-dial
button-layout 5-6 blf-speed-dial
overlap-signal
!
ephone 10
device-security-mode none
mac-address 02EA.EAEA.0010
overlap-signal
```

Example for Configuring Overlap Dialing for SIP IP Phones

The following example shows the **overlap-signal** configured in voice register global configuration mode and voice register pool 10:

```
Router# show running config
!
!
!
voice service voip
ip address trusted list
```

```
ipv4 20.20.20.1
media flow-around
allow-connections sip to sip
!
voice class media 10
media flow-around
!
!
voice register global
max-pool 10
overlap-signal
!
voice register pool 5
overlap-signal
!
!
!
```

Where to Go Next

After configuring system-level parameters, you are ready to configure phones for making basic calls in Cisco Unified CME.

- To use Extension Assigner to assign extension numbers to the phones in your Cisco Unified CME, see Create Phone Configurations Using Extension Assigner, on page 347.
- Otherwise, see Configure Phones to Make Basic Call, on page 315.

Feature Information for System-Level Parameters

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

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

Table 13: Feature Information for System-Level Parameters

Feature Name	Cisco Unified CME Versions	Feature Information
Redundant Router for SIP Phones	11.6	Introduces redundant router support for SIP phones.

Feature Name	Cisco Unified CME Versions	Feature Information
Unsolicited Notify for Shared Line and Presence Events for Cisco Unified SIP IP Phones	9.0	Allows the Unsolicited Notify mechanism to reduce network traffic during Cisco Unified SIP IP phone registration using the bulk registration method.
HFS Download Support for IP Phone Firmware and Configuration Files	8.8	Provides download support for SIP and SCCP IP phone firmware, scripts, midlets, and configuration files using the HTTP File-Fetch Server (HFS) infrastructure.
Bulk Registration	8.6/3.4	Introduces bulk registration support for SIP phones. Introduces bulk registration for registering a block of phone numbers with an external registrar.
Media Flow Around for SIP-SIP Trunks	8.5	Introduces the media flow around feature, which eliminates the need to terminate RTP and re-originate on Cisco Unified CME, reducing media switching latency and increasing the call handling capacity for Cisco Unified CME SIP trunk.
Overlap Dialing for SCCP and SIP Phones	8.5	Allows the dialed digits from the SIP or SCCP IP phones to pass across the PRI/BRI trunks as overlap digits and not as enbloc digits, enabling overlap dialing on the PRI/BRI trunks.
DSCP	7.1	Supports DSCP packet marking for Cisco Unified IP Phones to specify the class of service for each packet.
Maximum Ephones	7.0/4.3	The **max-ephones** command sets the maximum number of SCCP phones that can register to Cisco Unified CME, without limiting the number that can be configured. Maximum number of phones that can be configured is 1000.
Network Time Protocol for SIP Phones	4.1	Allows SIP phones to synchronize to an NTP server.

Feature Name	Cisco Unified CME Versions	Feature Information
Blocking Automatic Registration	4.0	Blocks IP phones that are not explicitly configured in Cisco Unified CME from registering.
Per-Phone Configuration Files and Alternate Location	4.0	Defines a location other than system for storing configuration files and specifies the type of configuration files to generate.
Redundant Router for SCCP Phones	4.0	Introduces redundant router capability.
SIP phones in Cisco Unified CME	3.4	Introduces support for SIP endpoints directly connected to Cisco Unified CME.

CHAPTER 7

Configuring Phones to Make Basic Calls

This chapter describes how to configure Cisco Unified IP phones in Cisco Unified Communications Manager Express (Cisco Unified CME) so that you can make and receive basic calls.

Caution The Interactive Voice Response (IVR) media prompts feature is only available on the IAD2435 when running IOS version 15.0(1)M or later.

Prerequisites for Configuring Phones to Make Basic Calls

- Cisco IOS software and Cisco Unified CME software, including phone firmware files for Cisco Unified IP phones to be connected to Cisco Unified CME, must be installed in router flash memory. See Install Cisco Unified CME Software, on page 105.

- For Cisco Unified IP phones that are running SIP and are connected directly to Cisco Unified CME, Cisco Unified CME 3.4 or a later version must be installed on the router. See Install Cisco Unified CME Software, on page 105.
- Procedures in Network Parameters, on page 121 and Configure System-Level Parameters, on page 167 must be completed before you start the procedures in this section.

Restrictions for Configuring Phones to Make Basic Calls

When you are configuring dial peers or ephone-dns, including park slots and conferencing extensions, on Cisco Integrated Services Router Voice Bundles, the following message may appear to warn you that free memory is not available:

%DIALPEER_DB-3-ADDPEER_MEM_THRESHOLD: Addition of dial-peers limited by available memory

To configure more dial peers or ephone-dns, increase the DRAM in the system. A moderately complex configuration may exceed the default 256 MB DRAM and require 512 MB DRAM. Note that many factors contribute to memory usage, in addition to the number of dial peers and ephone-dns configured.

Information About Configuring Phones to Make Basic Calls

Phones in Cisco Unified CME

An ephone, or “Ethernet phone,” for SCCP or a voice-register pool for SIP is the software configuration for a phone in Cisco Unified CME. This phone can be either a Cisco Unified IP phone or an analog phone. Each physical phone in your system must be configured as an ephone or voice-register pool on the Cisco Unified CME router to receive support in the LAN environment. Each phone has a unique tag, or sequence number, to identify it during configuration.

For information on the phones supported in Cisco Unified CME Release 8.8 and later versions, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Directory Numbers

A directory number, also known as an ephone-dn for SCCP or a voice-register dn for SIP, is the software configuration in Cisco Unified CME that represents the line connecting a voice channel to a phone. A directory number has one or more extension or telephone numbers associated with it to allow call connections to be made. Generally, a directory number is equivalent to a phone line, but not always. There are several types of directory numbers, which have different characteristics.

Each directory number has a unique *dn-tag*, or sequence number, to identify it during configuration. Directory numbers are assigned to line buttons on phones during configuration.

One virtual voice port and one or more dial peers are automatically created for each directory number, depending on the configuration for SCCP phones, or for SIP phones, when the phone registers in Cisco Unified CME.

Because each directory number represents a virtual voice port in the router, the number of directory numbers that you create corresponds to the number of simultaneous calls that you can have. This means that if you want more than one call to the same number to be answered simultaneously, you need multiple directory numbers with the same destination number pattern.

The directory number is the basic building block of a Cisco Unified CME system. Six different types of directory numbers can be combined in different ways for different call coverage situations. Each type will help with a particular type of limitation or call-coverage need. For example, if you want to keep the number of directory numbers low and provide service to a large number of people, you might use shared directory numbers. Or if you have a limited quantity of extension numbers that you can use and you need to have a large quantity of simultaneous calls, you might create two or more directory numbers with the same number. The key is knowing how each type of directory number works and its advantages.

Not all types of directory numbers can be configured for all phones or for all protocols. In the remaining information about directory numbers, we have used SCCP in the examples presented but that does not imply exclusivity. The following sections describe the types of directory numbers in a Cisco Unified CME system:

Single-Line

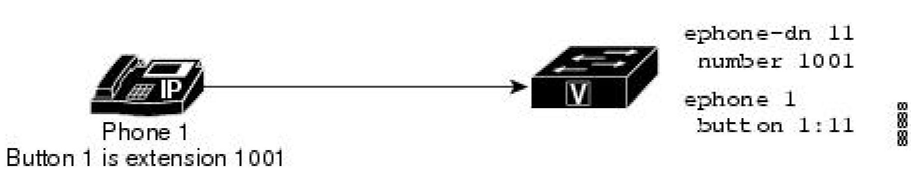
A single-line directory number has the following characteristics:

- Makes one call connection at a time using one phone line button. A single-line directory number has one telephone number associated with it.
- Should be used when phone buttons have a one-to-one correspondence to the PSTN lines that come into a Cisco Unified CME system.
- Should be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- Must have more than one single-line directory number on a phone when used with multiple-line features like call waiting, call transfer, and conferencing.
- Can be combined with dual-line directory numbers on the same phone.

Note You must make the choice to configure each directory number in your system as either dual-line or single-line when you initially create configuration entries. If you need to change from single-line to dual-line later, you must delete the configuration for the directory number, then recreate it.

Figure 6: Single-Line Directory Number, on page 225 shows a single-line directory number for an SCCP phone in Cisco Unified CME.

Figure 6: Single-Line Directory Number



Dual-Line

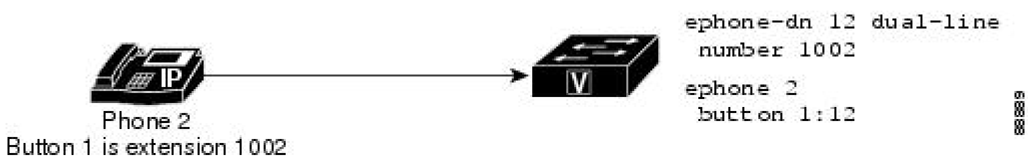
A dual-line directory number has the following characteristics:

- Has one voice port with two channels.
- Supported on IP phones that are running SCCP; not supported on IP phones that are running SIP.
- Can make two call connections at the same time using one phone line button. A dual-line directory number has two channels for separate call connections.
- Can have one number or two numbers (primary and secondary) associated with it.
- Should be used for a directory number that needs to use one line button for features like call waiting, call transfer, or conferencing.
- Cannot be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- Can be combined with single-line directory numbers on the same phone.

Note You must make the choice to configure each directory number in your system as either dual-line or single-line when you initially create configuration entries. If you need to change from single-line to dual-line later, you must delete the configuration for the directory number, then recreate it.

Figure 7: Dual-Line Directory Number, on page 226 shows a dual-line directory number for an SCCP phone in Cisco Unified CME.

Figure 7: Dual-Line Directory Number



Octo-Line

An octo-line directory number supports up to eight active calls, both incoming and outgoing, on a single button of a SCCP phone. Unlike a dual-line directory number, which is shared exclusively among phones (after a call is answered, that phone owns both channels of the dual-line directory number), an octo-line directory number can split its channels among other phones that share the directory number. All phones are allowed to initiate or receive calls on the idle channels of the shared octo-line directory number.

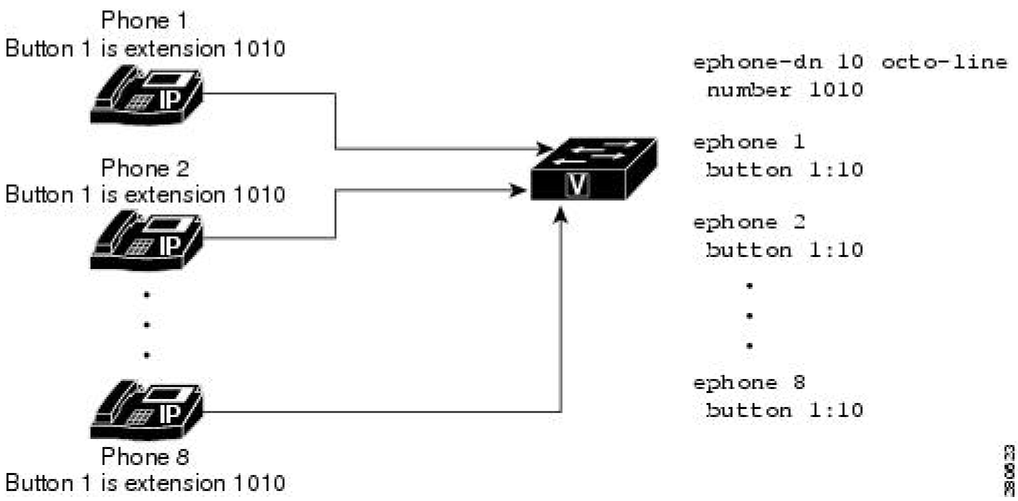
Because octo-line directory numbers do not require a different ephone-dn for each active call, one octo-line directory number can handle multiple calls. Multiple incoming calls to an octo-line directory number ring simultaneously. After a phone answers a call, the ringing stops on that phone and the call-waiting tone plays for the other incoming calls. When phones share an octo-line directory number, incoming calls ring on phones without active calls and these phones can answer any of the ringing calls. Phones with an active call hear the call-waiting tone.

After a phone answers an incoming call, the answering phone is in the connected state. Other phones that share the octo-line directory number are in the remote-in-use state.

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 user is in the process of initiating a call transfer or creating a conference, the call is locked and other phones that share the octo-line directory number cannot steal the call.

Figure 8: Octo-Line Directory Number, on page 227 shows an octo-line directory number for SCCP phones in Cisco Unified CME.

Figure 8: Octo-Line Directory Number



The Barge and Privacy features control whether other phones are allowed to view call information or join calls on the shared octo-line directory number.

Feature Comparison by Directory Number Line-Mode on SCCP Phones

Table 14: Feature Comparison by Line Mode on SCCP Phones , on page 227 lists some common directory number features and their support based on the type of line mode defined with the **ephone-dn** command.

Table 14: Feature Comparison by Line Mode on SCCP Phones

Feature	Single-Line	Dual-Line	Octo-Line
Barge	—	—	Yes
Busy Trigger	—	—	Yes
Conferencing (8-party)	—	4 directory numbers	1 directory number
FXO Trunk Optimization	Yes	Yes	—
Huntstop Channel	—	Yes	Yes
Intercom	Yes	—	—
Key System (one call per button)	Yes	—	—
Maximum Calls	—	—	Yes

Feature	Single-Line	Dual-Line	Octo-Line
MWI	Yes	—	—
Overlay directory numbers (c, o, x)	Yes	Yes	—
Paging	Yes	—	—
Park	Yes	—	—
Privacy	—	—	Yes

SIP Shared-Line (Nonexclusive)

Cisco Unified CME 7.1 and later versions support SIP shared lines to allow multiple phones to share a common directory number. All phones sharing the directory number can initiate and receive calls at the same time. Calls to the shared line ring simultaneously on all phones without active calls and any of these phones can answer the incoming calls. After a phone answers a call, the ringing stops on all phones and the call-waiting tone plays for other incoming calls to the connected phone.

The phone that answers an incoming call is in the connected state. Other phones that share the directory number are in the remote-in-use state. The first user that answers the call on the shared line is connected to the caller and the remaining users see the call information and status of the shared line.

Calls on a shared line can be put on hold like calls on a non-shared line. When a call is placed on hold, other phones with the shared-line directory number receive a hold notification so all phones sharing the line are aware of the held call. Any shared-line phone user can resume the held call. If the call is placed on hold as part of a conference or call transfer operation, the call cannot be resumed by other shared-line phone users. The ID of the held call is used by other shared-line members to resume the call. Notifications are sent to all associated phones when a held call is resumed on a shared line.

Shared lines support up to 16 calls, depending on the configuration in Cisco Unified CME, which rejects any new call that exceeds the configured limit. For configuration information, see Create Directory Numbers for SIP Phones, on page 263.

The Barge and Privacy features control whether other phones are allowed to view call information or join calls on the shared-line directory number. See Barge and Privacy, on page 1047.

Note When the **no supplementary-service sip handle-replaces** command is configured, SIP shared-line is not supported on CME.

Two Directory Numbers with One Telephone Number

Two directory numbers with one telephone or extension number have the following characteristics:

- Have the same telephone number but two separate virtual voice ports, and therefore can have two separate call connections.

- Can be dual-line (SCCP only) or single-line directory numbers.
- Can appear on the same phone on different buttons or on different phones.
- Should be used when you want the ability to make more call connections while using fewer numbers.

Figure 9: Two Directory Numbers with One Number on One Phone, on page 230 shows a phone with two buttons that have the same number, extension 1003. Each button has a different directory number (button 1 is directory number 13 and button 2 is directory number 14), so each button can make one independent call connection if the directory numbers are single-line and two call connections (for a total of four) if the directory numbers are dual-line.

Figure 10: Two Directory Numbers with One Number on Two Phones, on page 230 shows two phones that each have a button with the same number. Because the buttons have different directory numbers, the calls that are connected on these buttons are independent of one another. The phone user at phone 4 can make a call on extension 1003, and the phone user on phone 5 can receive a different call on extension 1003 at the same time.

The two directory numbers-with-one-number situation is different than a shared line, which also has two buttons with one number but has only one directory number for both of them. A shared directory number will have the same call connection at all the buttons on which the shared directory number appears. If a call on a shared directory number is answered on one phone and then placed on hold, the call can be retrieved from the second phone on which the shared directory number appears. But when there are two directory numbers with one number, a call connection appears only on the phone and button at which the call is made or received. In the example in Figure 10: Two Directory Numbers with One Number on Two Phones, on page 230, if the user at phone 4 makes a call on button 1 and puts it on hold, the call can be retrieved only from phone 4. For more information about shared lines, see Shared Line (Exclusive), on page 231 section.

The examples in Figure 9: Two Directory Numbers with One Number on One Phone, on page 230 and Figure 10: Two Directory Numbers with One Number on Two Phones, on page 230 show how two directory numbers with one number are used to provide a small hunt group capability. In Figure 9: Two Directory Numbers with One Number on One Phone, on page 230, if the directory number on button 1 is busy or does not answer, an incoming call to extension 1003 rolls over to the directory number associated with button 2 because the appropriate related commands are configured. Similarly, if button 1 on phone 4 is busy, an incoming call to 1003 rolls over to button 1 on phone 5.

Figure 9: Two Directory Numbers with One Number on One Phone

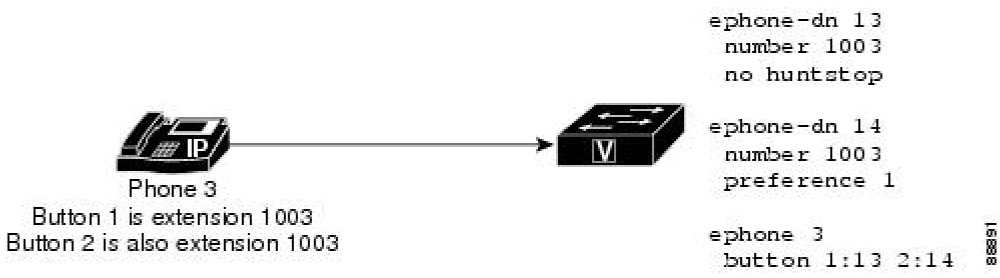
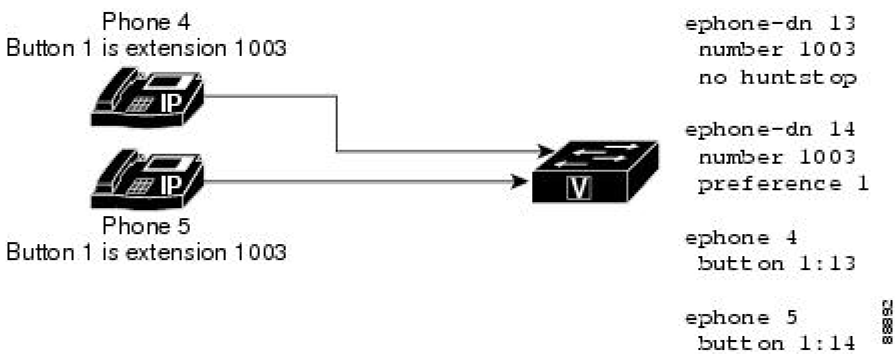


Figure 10: Two Directory Numbers with One Number on Two Phones



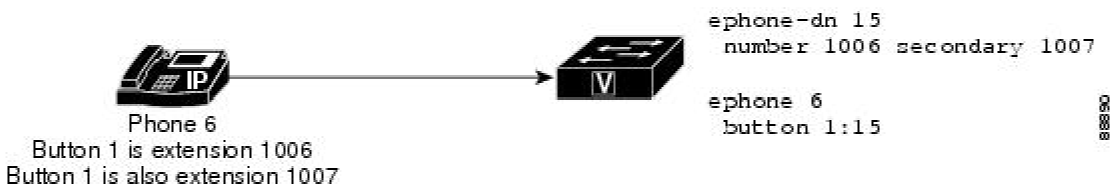
Dual-Number

A dual-number directory number has the following characteristics:

- Has two telephone numbers, a primary number and a secondary number.
- Can make one call connection if it is a single-line directory number.
- Can make two call connections at a time if it is a dual-line directory number (SCCP only).
- Should be used when you want to have two different numbers for the same button without using more than one directory number.

Figure 11: Dual-Number Directory, on page 231 shows a directory number that has two numbers, extension 1006 and extension 1007.

Figure 11: Dual-Number Directory



Shared Line (Exclusive)

An exclusively shared directory number has the following characteristics:

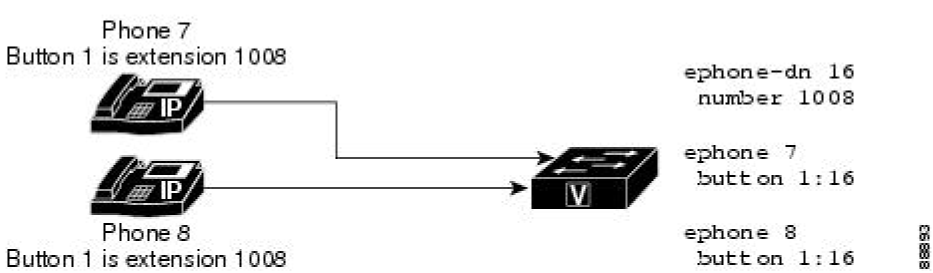
- Has a line that appears on two different phones but uses the same directory number, and extension or phone number.
- Can make one call at a time and that call appears on both phones.
- Should be used when you want the capability to answer or pick up a call at more than one phone.

Because this directory number is shared exclusively among phones, if the directory number is connected to a call on one phone, that directory number is unavailable for calls on any other phone. If a call is placed on hold on one phone, it can be retrieved on the second phone. This is like having a single-line phone in your house with multiple extensions. You can answer the call from any phone on which the number appears, and you can pick it up from hold on any phone on which the number appears.

Note Transcoding is not supported for Shared Lines.

Figure 12: Shared Directory Number (Exclusive), on page 231 shows a shared directory number on phones that are running SCCP. Extension 1008 appears on both phone 7 and phone 8.

Figure 12: Shared Directory Number (Exclusive)



Mixed Shared Lines

Cisco Unified CME 9.0 and later versions support the mixed Cisco Unified SIP/SCCP shared line. This feature allows Cisco Unified SIP and SCCP IP phones to share a common directory number.

The mixed shared line supports up to 16 calls, depending on the configuration in Cisco Unified CME, which rejects any new call that exceeds the configured limit.

For configuration information, see Create Directory Numbers for SCCP Phones, on page 253 and Create Directory Numbers for SIP Phones, on page 263.

Incoming and Outgoing Calls

All phones sharing the common directory number can initiate and receive calls at the same time. Calls to the mixed shared line ring simultaneously on all phones without active calls and any of these phones can answer the incoming calls. After a phone answers a call, the ringing stops on all phones and the call-waiting tone plays for other incoming calls to the connected phone.

The phone that answers an incoming call is in the connected state. Other phones that share the common directory number are in the remote-in-use state. The first user who answers the call on the mixed shared line is connected to the caller and the remaining users see the call information and status of the mixed shared line.

When a mixed shared-line user makes an outgoing call on the shared line, all the other shared-line users are notified of the outgoing call. When the called party answers, the caller is connected while the remaining shared-line users see the call information and the status of the call on the mixed shared line.

Hold and Resume

Calls on a mixed shared line can be put on hold like calls on a non-shared line. When a call is placed on hold, other phones with the shared-line directory number receive a hold notification so all phones sharing the line are aware of the call on hold. Any shared-line phone user can resume the call on hold. The ID of the call on hold is used by other shared-line members to resume the call. Notifications are sent to all associated phones when a call on hold is resumed on a mixed shared line. If the call is placed on hold as part of a conference or call transfer operation, the resume feature is not allowed.

Privacy on Hold

The Privacy on Hold feature prevents other phone users from viewing call information or retrieving a call put on hold by another phone sharing a common directory number. Only the caller who put the call on hold can see the status of the held call.

By default, Privacy on Hold feature is disabled for all phones on a shared line. Use the **privacy-on-hold** command in telephony-service configuration mode to enable the Privacy feature for calls that are on hold on Cisco Unified SCCP IP phones on a mixed shared line. Use the **privacy-on-hold** command in voice register global configuration mode to enable the Privacy feature for calls that are on hold on Cisco Unified SIP IP phones on a mixed shared line.

The **no privacy** and **privacy off** commands override the **privacy-on-hold** command.

Call Transfer and Forwarding

Both blind transfer and consult transfer are supported on a mixed shared line. A mixed shared line can be the one transferring the call, the one receiving the transferred call, or the call being transferred.

There are four types of call forwarding: all calls, no answer, busy, and night service. Any of these can be configured under a shared SCCP ephone-dn or a shared SIP voice register dn. However, the user must keep the call forwarding parameters for the SCCP and SIP lines synchronized with each other. A mixed shared line can be the one forwarding the call, the one receiving the forwarded call, or the call being forwarded.

For more information, see Configure Call Transfer and Forwarding, on page 1178.

Call Pickup

The Call Pickup feature is supported on a mixed shared line when the **call-park system application** command is configured in telephony-service configuration mode.

A user can answer a call that:

- Originates from a shared line
- Rings on a shared line
- Originates from one shared line and rings on another shared line

For more information, see Call Pickup, on page 1243.

Call Park

The Call Park feature is supported on a mixed shared line when the **call-park system application** command is configured in telephony-service configuration mode.

For more information, see Call Park, on page 1081.

Message Waiting Indication

SCCP and SIP message-waiting indication (MWI) services are supported on Cisco Unity and Cisco Unity voice mails on mixed shared lines:

The following are two ways of registering a mixed shared line for an MWI service from a SIP-based MWI server with the shared-line option:

- Configure the **mwi sip** command in ephone-dn or ephone-dn-template configuration mode.
- Configure the **mwi** command in voice register dn configuration mode.

For SCCP MWI service on a mixed shared line, use the **mwi** {**off** |**on** | **on-off**} command in ephone-dn configuration mode to enable a specific Cisco Unified IP phone extension to receive MWI notification from an external voice-messaging system.

Software Conferencing

A local software conference can be created on a mixed shared line, with the mixed shared line acting as a conference creator and a conference participant.

For software conferencing on a mixed shared line, other shared-line users remain in remote-in-use state and do not see the calls on hold when the conference call is put on hold by a mixed-shared-line user acting as the conference creator.

Note Only the conference creator, who put a conference call on hold, can resume the conference call.

Dial Plan

A dial plan pattern enables abbreviated extensions to be expanded into fully qualified E.164 numbers and builds additional dial peers for the expanded numbers it creates.

Features are effectively supported on a mixed shared line when dial-plan patterns have matching configurations in telephony-service and voice register global configuration modes using the **dialplan pattern** command.

Busy Lamp Field Speed-Dial Monitoring

A mixed shared line only supports directory number-based Busy-Lamp-Field (BLF) Speed-Dial monitoring and not device-based monitoring.

Restrictions For Mixed Shared Lines

The following features are not supported on mixed Cisco Unified SIP/SCCP shared lines:

- Privacy
- Barge
- cBarge
- Single Number Reach
- Hardware Conferencing
- Remote-resume on a local software conference call
- Video calls
- Overlay DNs on Cisco Unified SCCP IP phones
- Features in the CTI CSTA protocol suite

Overlaid Directory Numbers

An overlaid directory number has the following characteristics:

- Is a member of an overlay set, which includes all the directory numbers that have been assigned together to a particular phone button.
- Can have the same telephone or extension number as other members of the overlay set or different numbers.
- Can be single-line or dual-line, but cannot be mixed single-line and dual-line in the same overlay set.
- Can be shared on more than one phone.

Overlaid directory numbers provide call coverage similar to shared directory numbers because the same number can appear on more than one phone. The advantage of using two directory numbers in an overlay arrangement rather than as a simple shared line is that a call to the number on one phone does not block the use of the same number on the other phone, as would happen if it were a shared directory number.

For information about configuring call coverage using overlaid ephone-dns, see Configure Call Coverage Features, on page 1278.

You can overlay up to 25 lines on a single button. A typical use of overlaid directory numbers would be to create a "10x10" shared line, with 10 lines in an overlay set shared by 10 phones, resulting in the possibility of 10 simultaneous calls to the same number. For configuration information, see Creating Directory Numbers for a Simple Key System on SCCP Phone, on page 282.

Auto Registration of SIP Phones on Cisco Unified CME

Cisco Unified CME supports auto registration of both SIP and SCCP phones. When the auto registration feature is enabled, the **voice register pool** and **voice register dn** commands do not need to be manually configured for the phones. The configuration is automatically created when the phone registers.

The auto registration feature for SIP phones is enabled with the **auto-register** command under **voice register global** configuration mode. For more information on auto-register command, see Cisco Unified Communications Manager Express Command Reference.

The auto registration of SCCP phones is enabled with the **auto-reg-ephone** command under **telephony-service** configuration mode. For more information on auto-register command, see Cisco Unified Communications Manager Express Command Reference.

As part of the **auto-register** command, certain CLI sub-mode configuration options are available to the administrator to successfully register phones using auto-registration on Unified CME.

```
Router(config-register-global)#auto-register
Router(config-voice-auto-register)#
Router(config-voice-auto-register)# ?
VOICE auto register configuration commands:
  auto-assign     Define DN range for auto assignment
  default         Set a command to its defaults
  exit            Exit from voice register group configuration mode
  no              Negate a command or set its defaults
  password        Default password for auto-register phones
  service-enable  Enable SIP phone Auto-Registration
  template        Default template for auto-register phones
```

For details on the configuration steps for auto registration of SIP phones, see Configure Auto Registration for SIP Phones, on page 315.

Service Enable **—**If the administrator needs to temporarily disable or enable auto registration without losing configurations such as DN range, and password, the no form of the CLI option **service-enable** is used (**no service-enable**). Once **auto-register** command is entered, the service is enabled by default. To re-enable the auto registration feature, use the command **service-enable**. It is a sub-mode option in the CLI command **auto-register**. To disable auto registration including removal of configurations such as password and DN range, the **no** form of the CLI command **auto-register** (under voice register global) is used.

```
Router(config)#voice register global
Router(config-register-global)#auto-register
Router(config-voice-auto-register)#no service-enable ?
<cr>
```

Password **—**As part of the auto registration feature, authentication of phones registering on Unified CME is enabled. When the phone registers with Unified CME, it is mandatory for the administrator to configure the password credentials; username is assigned by default. However, the administrator can modify the username and password credentials under the corresponding voice register pool that gets created after auto registration.

```
Router(config)#voice register global
Router(config-register-global)#auto-register
Router(config-voice-auto-register)#password ?
  WORD  Password string
```

Note It is mandatory that **password** is configured before DN range (auto-assign) while registering phones using auto registration.

Auto Assign —It is mandatory to define a directory number (DN) range for auto-registration feature to work. The DN range that can be assigned to phones registering on Unified CME is configured using **auto-assign** <**first-dn**> **to** <**last-dn**>, which is a submode option of the CLI command **auto-register** (under **voice register global**). The DN numbers assigned to the phones through auto registration are always within the DN range that is defined. However, ensure that the defined DN range is within the maximum DNs recommended for the supported platform.

```
Router(config)#voice register global
Router(config-register-global)#auto-register
Router(config-voice-auto-register)#auto-assign ?
  <1-4294967295>  First DN number
Router(config-voice-auto-register)#auto-assign 1001 ?
  <1-4294967295>  Last DN number
Router(config-voice-auto-register)#auto-assign 1001 to 1010
```

The automatic registration feature also provides the administrators with the option to enhance a predefined DN range. The enhancement of an existing DN range is supported such that the new first-dn is not greater that the existing first-dn and the new last-dn is not less than the existing last-dn.

For example, the DN range 8001-8006 can be enhanced as 7999-8006, 8000-8007, but not as 8002-8006 or 8001 to 8005.

```
Router# show running-config | section voice register global
  voice register global
   mode cme
   source-address 8.41.20.1 port 5060
     auto-register
        password xxxx
       auto-assign 8001 to 8006
   max-dn 50
   max-pool 40
  Router(config-register-global)#auto-assign 8002 to 8006
  Start DN should not be greater than existing First DN
  Router(config-register-global)#auto-assign 8001 to 8005
  Stop DN should not be less than existing Last DN
```

The DN assigned to phone using the auto registration feature does not duplicate a manually configured DN. When the defined DN range includes a previously registered DN, that DN is skipped as part of the auto registration process. However, when a previously registered DN deregisters and the corresponding configuration for the DN and pool are removed, it can be assigned to a phone registering on Unified CME using auto registration. The assignment of DN range is done in round robin fashion and the first available free DN is assigned to the phone that is auto registering with Unified CME.

Note We recommend that administrators choose different DN ranges for manually configured and auto configured phones.

Template —Administrators are provided the option to create a basic configuration template that can be applied to all phones registering automatically on Unified CME. This basic configuration template supports all the configurations currently supported by the voice register template. It is mandatory that voice register template is configured with the same template tag.

```
Router(config)#voice register global
Router(config-register-global)#auto-register
Router(config-voice-auto-register)#template ?
```

```
  <1-10>  template tag>
Router(config-voice-auto-register)#template 10
```

All phone configurations such as voice-register-pool and voice-register-dn that are generated as part of the auto registration process are persistent configurations. These configurations will be available on the Unified CME even after an event of router reload.

The CLI commands show **voice register pool** all and **show voice register pool all brief** distinctly mention the registration process for phones as registered or unregistered for manual registration, and registered* or unregistered* for automatic registration. However, the registration status for auto-registered phones are reset in the event of a router reload. Then, phone registration status displays only as registered or unregistered.

Syslog Messages

Unified CME generates Syslog messages as part of the auto registration feature, when the phone registers and unregisters with the Cisco Unified CME. Also, based on the DN range configured, the administrator gets syslog message providing updates on the registration status of assigned DNs. The syslog messages that provide updates are generated at two instances; at 80% utilization of available DNs, and at 100% utilization of DNs.

The Unified CME system generates the following syslog messages as part of auto registration.

- Syslog message when phone registers with Unified CME:

```
*Mar 28 21:44:08.795 IST: %SIPPHONE-6-REGISTER: VOICE REGISTER POOL-8 has registered.
 Name:SEP2834A2823843  IP:8.41.20.58 DeviceType:Phone
```

- Syslog message at 80% utilization of DN range:

```
*Mar 28 21:42:25.732 IST: %SIPPHONE-6-AUTOREGISTER80: AUTO-REGISTER: 80% of DN range
is consumed
```

- Syslog message at 100% utilization of DN range:

```
*Mar 28 21:44:03.328 IST: %SIPPHONE-6-AUTOREGISTER100: AUTO-REGISTER: 100% of DN range
 is consumed
```

- Syslog message when phone unregisters with Unified CME:

```
*Mar 28 18:03:41.748 IST: %SIPPHONE-6-UNREGISTER: VOICE REGISTER POOL-6 has unregistered.
 Name:SEPB000B4BAF3DA  IP:8.41.20.53  DeviceType:Phone
```

Monitor Mode for Shared Lines

In Cisco CME 3.0 and later versions, monitor mode for shared lines provides a visible line status indicating whether the line is in-use or not. A monitor-line lamp is off or unlit only when its line is in the idle call state. The idle state occurs before a call is made and after a call is completed. For all other call states, the monitor line lamp is lit. A receptionist who monitors the line can see that it is in use and can decide not to send additional calls to that extension, assuming that other transfer and forwarding options are available, or to report the information to the caller; for example, “Sorry, that extension is busy, can I take a message?”

In Cisco CME 3.2 and later versions, consultative transfers can occur during Direct Station Select (DSS) for transferring calls to idle monitored lines. The receptionist who transfers a call from a normal line can press the Transfer button and then press the line button of the monitored line, causing the call to be transferred to the phone number of the monitored line. For information about consultative transfer with DSS, see Configure Call Transfer and Forwarding, on page 1178.

In Cisco Unified CME 4.0(1) and later versions, the line button for a monitored line can be used as a DSS for a call transfer when the monitored line is idle or in-use, provided that the call transfer can succeed; for example, when the monitored line is configured for Call Forward Busy or Call Forward No Answer.

Note Typically, Cisco Unified CME does not attempt a transfer that causes the caller (transferee) to hear a busy tone. However, the system does not check the state of subsequent target numbers in the call-forward path when the transferred call is transferred more than once. Multiple transfers can occur because a call-forward-busy target is also busy and configured for Call Forward Busy.

In Cisco Unified CME 4.3 and later versions, a receptionist can use the Transfer to Voicemail feature to transfer a caller directly to a voice-mail extension for a monitored line. For configuration information, see Transfer to Voice Mail, on page 551.

For configuration information for monitor mode, see Create Directory Numbers for SCCP Phones, on page 253.

Monitor mode is intended for use only in the context of shared lines so that a receptionist can visually monitor the in-use status of several users' phone extensions; for example, for Busy Lamp Field (BLF) notification. To monitor all lines on an individual phone so that a receptionist can visually monitor the in-use status of that phone, see Watch Mode for Phones, on page 238.

For BLF monitoring of speed-dial buttons and directory call-lists, see Configure Presence Service, on page 879.

Watch Mode for Phones

In Cisco Unified CME 4.1 and later versions, a line button that is configured for watch mode on one phone provides BLF notification for all lines on another phone (watched phone) for which watched directory number is the primary line. Watch mode allows a phone user, such as a receptionist, to visually monitor the in-use status of an individual phone. A user can use the line button that has been set in watch mode as a speed-dial to call the first extension of the watched phone. The watching phone button displays a red light when the watched phone is unregistered in a DND state or in an offhook state. Pressing the button when it is not displaying a red light will dial the number in the same manner it would for a monitor button or the speed-dial button. Incoming calls on a line button that is in watch mode do not ring and do not display caller ID or call-waiting caller ID.

The line button for a watched phone can also be used as a DSS for a call transfer when the watched phone is idle. In this case, the phone user who transfers a call from a normal line can press the Transfer button and then press the line button of the watched directory number, causing the call to be transferred to the phone number associated with the watched directory number.

For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

If the watched directory number is a shared line and the shared line is not idle on any phone with which it is associated, then in the context of watch mode, the status of the line button indicates that the watched phone is in use.

For best results when monitoring the status of an individual phone based on a watched directory number, the directory number configured for watch mode should not be a shared line. To monitor a shared line so that a receptionist can visually monitor the in-use status of several users' phone extensions, see Monitor Mode for Shared Lines, on page 237.

For BLF monitoring of speed-dial buttons and directory call-lists, see Presence Service, on page 875.

PSTN FXO Trunk Lines

In Cisco CME 3.2 and later versions, IP phones running SCCP can be configured to have buttons for dedicated PSTN FXO trunk lines, also known as FXO lines. FXO lines may be used by companies whose employees require private PSTN numbers. For example, a salesperson may need a special number that customers can call without having to go through a main number. When a call comes in to the direct number, the salesperson knows that the caller is a customer. In the salesperson's absence, the customer can leave a voice mail. FXO lines can use PSTN service provider voice mail: when the line button is pressed, the line is seized, allowing the user to hear the stutter dial tone provided by the PSTN to indicate that voice messages are available.

Because FXO lines behave as private lines, users do not have to dial a prefix, such as 9 or 8, to reach an outside line. To reach phone users within the company, FXO-line users must dial numbers that use the company's PSTN number. For calls to non-PSTN destinations, such as local IP phones, a second directory number must be provisioned.

Calls placed to or received on an FXO line have restricted Cisco Unified CME services and cannot be transferred by Cisco Unified CME. However, phone users are able to access hookflash-controlled PSTN services using the Flash softkey.

In Cisco Unified CME 4.0(1), the following FXO trunk enhancements were introduced to improve the keyswitch emulation behavior of PSTN lines on phones running SCCP in a Cisco Unified CME system:

- FXO port monitoring—Allows the line button on IP phones to reliably show the status of an FXO port when the port is in use. The status indicator, either a lamp or an icon, depending on the phone model, accurately displays the status of the FXO port during the duration of the call, even after the call is forwarded or transferred. The same FXO port can be monitored by multiple phones using multiple trunk ephone-dns.
- Transfer recall—If a transfer-to phone does not answer after a specified timeout, the call is returned to the phone that initiated the transfer and it resumes ringing on the FXO line button. The directory number must be dual-lined.
- Transfer-to button optimization—When an FXO call is transferred to a private extension button on another phone, and that phone has a shared line button for the FXO port, after the transfer is committed and the call is answered, the connected call displays on the FXO line button of the transfer-to phone. This frees up the private extension line on the transfer-to phone. The directory number *n* must be dual-line.
- Dual-line ephone-dns— Directory numbers for FXO lines can now be configured for dual-line to support the FXO monitoring, transfer recall, and transfer-to button optimization features.

For configuration information, see Configure Trunk Lines for a Key System on SCCP Phone, on page 284.

Codecs for Cisco Unified CME Phones

In Cisco CME 3.4, support for connecting and provisioning SIP phones was added. The default codec of the POTS dial peer for an SCCP phone is G.711 and the default codec of a VoIP dial peer for a SIP phone is G.729. If neither the SCCP phone nor the SIP phone in Cisco Unified CME is specifically configured to change the codec, calls between the two phones on the same router will produce a busy signal caused by the mismatched default codecs. To avoid codec mismatch, specify the codec for individual IP phones in Cisco Unified CME. Modify the configuration for either SIP or SCCP phones to ensure that the codec for all phones match. Do not modify the configuration for both SIP and SCCP phones. For configuration information, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.

In Cisco Unified CME 4.3, support for G.722-64K and the Internet Low Bit Rate Codec (iLBC) was added. This enables Cisco Unified CME to support the same codecs that are used in newer Cisco Unified IP phones, mobile wireless networks, and internet telephony without transcoding. This feature provides support for the following:

- iLBC and G.722-capable SIP and SCCP IP phones in Cisco Unified CME.
- iLBC-capable SCCP analog endpoints and remote phones in Cisco Unified CME.
- Conferencing support for G.722 and ILBC.
- Supplementary services, such as transfer, call forward, MOH, support for G.722 and iLBC, including any supplementary services that require transcoding between G.722 and any other codec.
- Transcoding for G.722 and iLBC, including G.722 to G.711 and G.722 to any other codec.

With the introduction of G.722 and iLBC codecs, there can be a disparity between codec capabilities of different phones and different firmware versions on same phone type. For example, when a H.323 call is established, the codec is negotiated based on the dial-peer codec and the assumption is that the codecs supported on H.323 side are supported by the phones. This assumption is not valid after G.722 and ILBC codec are introduced in your network. If the phones do not support the codecs on the H.323 side, a transcoder is required. To avoid transcoding in this situation, configure incoming dial-peers so that G.722 and iLBC codecs are not used for calls to phones that are not capable of supporting these codecs. Instead, configure these phones for G.729 or G.711. Also, when configuring shared directory numbers, ensure that phones with the same codec capabilities are connected to the shared directory number.

G.722-64K

Traditional PSTN telephony codecs, including G.711 and G.729, are classified as narrowband codecs because they encode audio signals in a narrow audio bandwidth, giving telephone calls a characteristic “tinny” sound. Wideband codecs, such as G.722, provide a superior voice experience because wideband frequency response is 200 Hz to 7 kHz compared to narrowband frequency response of 300 Hz to 3.4 kHz. At 64 kbps, the G.722 codec offers conferencing performance and good music quality.

A wideband handset for certain Cisco Unified IP phones, such as the Cisco Unified IP Phone 7906G, 7911G, 7941G-GE, 7942G, 7945G, 7961G-GE, 7962G, 7965G, and 7975G, take advantage of the higher voice quality provided by wideband codecs to enhance end-user experience with high-fidelity wideband audio. When users use a headset that supports wideband, they experience improved audio sensitivity when the wideband setting on their phones is enabled. You can configure phone-user access to the wideband headset setting on IP phones by setting the appropriate VendorConfig parameters in the phone’s configuration file. For configuration information, see Modify Cisco Unified IP Phone Options, on page 1437.

If the system is not configured for a wideband codec, phone users may not detect any additional audio sensitivity, even when they are using a wideband headset.

You can configure the G.722-64K codec at a system-level for all calls through Cisco Unified CME. For configuration information, see Modify the Global Codec, on page 278. To configure individual phones and avoid codec mismatch for calls between local phones, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.

iLBC codec

Internet Low Bit Rate Codec (iLBC) enables graceful speech quality degradation in a network where frames get lost. Consider iLBC suitable for real-time communications, such as telephony and video conferencing, streaming audio, archival, and messaging. This codec is widely used by internet telephony softphones.The SIP, SCCP, and MGCP call protocols support use of the iLBC as an audio codec. iLBC provides better voice quality than G.729 but less than G.711. Supporting codecs that have standardized use in other networks, such as iLBC, enables end-to-end IP calls without the need for transcoding.

To configure individual SIP or SCCP phones, including analog endpoints in Cisco Unified CME, and avoid codec mismatch for calls between local phones, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.

Analog Phones

Cisco Unified CME supports analog phones and fax machines using Cisco Analog Telephone Adaptors (ATAs) or FXS ports in SCCP, H.323 mode, and fax pass-through mode. The FXS ports used for analog phones or fax can be on a Cisco Unified CME router, Cisco VG224 voice gateway, or integrated services router (ISR).

This section provides information on the following topics:

Cisco ATAs in SCCP Mode

You can configure the Cisco ATA 186 or Cisco ATA 188 to cost-effectively support analog phones using SCCP in Cisco IOS Release 12.2(11)T and later versions. Each Cisco ATA enables two analog phones to function as IP phones. For configuration information, see Configure Cisco ATA Support, on page 295.

FXS Ports in SCCP Mode

FXS ports on Cisco VG224 Voice Gateways and Cisco 2800 Series and Cisco 3800 Series ISRs can be configured for SCCP supplementary features. For information about using SCCP supplementary features on analog FXS ports on a Cisco IOS gateway under the control of a Cisco Unified CME router, see Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

FXS Ports in H.323 Mode

FXS ports on platforms that cannot enable SCCP supplementary features can use H.323 mode to support call waiting, caller ID, hookflash transfer, modem pass-through, fax (T.38, Cisco fax relay, and pass-through), and PLAR. These features are provisioned as Cisco IOS voice features and not as Cisco Unified CME features.

Note When using Cisco Unified CME, you can configure FXS ports in H.323 mode for call waiting or hookflash transfer, but not both at the same time.

Fax Support

Cisco Unified CME 4.0 introduced the use of G.711 fax pass-through for SCCP on the Cisco VG224 voice gateway and Cisco ATA. In Cisco Unified CME 4.0(3) and later versions, fax relay using the Cisco-proprietary fax protocol is the only supported fax option for SCCP-controlled FXS ports on the Cisco VG224 and integrated service routers. For more information on fax relay, see Fax Relay, on page 749.

Cisco ATA-187

Cisco Unified CME 9.0 and later versions provide voice and fax support on Cisco ATA-187.

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

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

For information on how to configure voice and fax support on Cisco ATA-187, see Configure Voice and T.38 Fax Relay on Cisco ATA-187, on page 298.

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

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

Cisco VG202, VG204, and VG224 Auto Configuration

The Auto Configuration feature in Cisco Unified CME 7.1 and later versions allows you to automatically configure the Cisco VG202, VG204, and VG224 Analog Phone Gateway. You can configure basic voice gateway information in Cisco Unified CME, which then generates XML configuration files for the gateway and saves the files to either the default location in system:/its/ or to a location you define in system memory, flash memory, or an external TFTP server. When the voice gateway powers up, it downloads the configuration files from Cisco Unified CME and based on the information in the files, the voice gateway provisions its analog voice ports and creates the corresponding dial peers.

Using this Auto Configuration feature with the existing Auto Assign feature allows you to quickly set up analog phones to make basic calls. After the voice gateway is properly configured and it downloads its XML configuration files from Cisco Unified CME, the SCCP telephony control (STC) application registers each configured voice port to Cisco Unified CME.

If you enable the Auto Assign feature, the gateway automatically assigns the next available directory number from the pool set by the **auto assign** command, binds that number to the requesting voice port, and creates an ephone entry associated with the voice port. The MAC address for the ephone entry is calculated based on the MAC address of the gateway and the port number. You can manually assign a directory number to each of the voice ports by creating the ephone-dn and corresponding ephone entry.

You can initiate a reset or restart of the analog endpoints from Cisco Unified CME, which triggers the autoconfiguration process. The voice gateway downloads its configuration files from Cisco Unified CME and applies the new changes.

For configuration information, see Auto-Configuration for Cisco VG202, VG204, and VG224, on page 302.

Internet Protocol - Secure Telephone Equipment Support

Cisco Unified CME 8.0 adds support for a new secure endpoint, Internet Protocol - Secure Telephone Equipment (IP-STE). IP-STE is a standalone, V.150.1 capable device which functions like a 7960 phone with secure communication capability. IP-STE has native state signaling events (SSE / SPRT) support and supports SCCP protocol. IP-STE uses the device ID 30035 when registering to a SCCP server. However, only V.150.1 modem relay is implemented in an IP-STE stack and V150.1 modem passthrough is not supported. Therefore, the response to capability query from Cisco Unified CME only includes media_payload_XV150_MR_711U and media_payload_xv150_MR_729A.

For configuration information, see Configure Secure IP Phone (IP-STE) on SCCP Phone, on page 311.

The following support is added for IP-STE endpoints:

- The IP-STE endpoint allows secure communication between gateway-connected legacy analog STE/STU devices and IP STE devices using existing STE devices in voice networks.
- Secure voice and secure data modes from STE/STU devices connected to Cisco IOS gateway foreign exchange station (FXS) and BRI ports to an IP-STE.
- Support for the state signaling events (SSE) protocol, allowing for modem signaling end-to-end and VoIP to modem over IP (MoIP) transition and operation.
- Interoperation between line-side and trunk-side gateways and Cisco Unified CME to determine codec support and V.150.1 negotiation. You can configure gateway-attached devices to support either modem relay, modem pass-through, both modem transport methods, or neither method.

Secure Communications Between STU, STE, and IP-STE

Secure Telephone Equipment (STE) and Secure Telephone Units (STUs) encrypt voice and data streams with government proprietary algorithms (Type-1 encryption). To provide support for the legacy STEs and STUs and next generation IP Secure Telephone Equipment (IP-STE), voice gateways must be able to support voice and data in secure mode within the IP network and be able to pass calls within and also to and from government voice networks.

In earlier versions of Cisco Unified CME, Cisco IOS gateways supported secure voice and data communication between legacy STE and STU devices using modem pass-through method. Cisco Unified CME 8.0 and later versions control the secure endpoints by implementing a subset of v.150.1 modem relay protocol and ensures secure communications between IP-STE endpoints and STE/STU endpoints. This allows Cisco Unified CME SCCP controlled secure endpoints to communicate with the IP-STE or legacy endpoints in secure mode.

SCCP Media Control for Secure Mode

IP-STE endpoints use the V.150.1 modem relay transport method using Future Narrow Band Digital Terminal (FNBDT) signaling over a V.32 or V.34 data pump for secure communication with other legacy STE endpoints. However, IP-STE endpoints cannot communicate with STU endpoints because STU endpoints use the modem pass-through method using a proprietary data pump and do not support the FNBDT signaling.

Secure communication between IP-STE endpoints and legacy STE endpoints support the following encryption-capable endpoints:

- STE—Specialized encryption-capable analog or BRI phones that can communicate over V.150.1 modem relay or over modem pass-through, also known as Voice Band Data (VBD).
- IP-STE—Specialized encryption-capable IP phones that communicate only over V.150.1 modem relay.
- STU—Specialized encryption-capable analog phones that operate only over NSE-based modem pass-through connections.

Table 15: Supported Secure Call Scenarios and Modem Transport Methods , on page 244 lists call scenarios between devices along with modem transport methods that the IP-STE endpoints use to communicate with STE endpoints.

Table 15: Supported Secure Call Scenarios and Modem Transport Methods

Device Type	STU	STE	IP-STE
STU	Pass-through	Pass-through	None
STE	Pass-through	Pass-through	Relay
IP-STE	None	Relay	Relay

Secure Communication Between STE, STU, and IP-STE Across SIP Trunk

The Secure Device Provisioning (SDP) for SIP end-to end negotiation includes four proprietary media types for secure communication between Cisco Unified CME and SIP trunk. These proprietary VBD or Modem Relay (MR) media types can be encoded into media attributes of SDP media lines. VBD capabilities are signaled using the SDP extension mechanism and Cisco proprietary nomenclature. MR capabilities are signaled through V.150.1. The following example shows VBD capabilities. The SDP syntax are based on RFC 2327 and V.150.1 Appendix E.

```
a=rtpmap:100 X-NSE/8000
a=rtpmap:118 v150fw/8000
a=sqn:0
a=cdsc:1 audio RTP/AVP 118 0 18
a=cdsc: 4 audio udsprt 120
a=cpar: a=sprtmap: 120 v150mr/8000
```

Remote Teleworker Phones

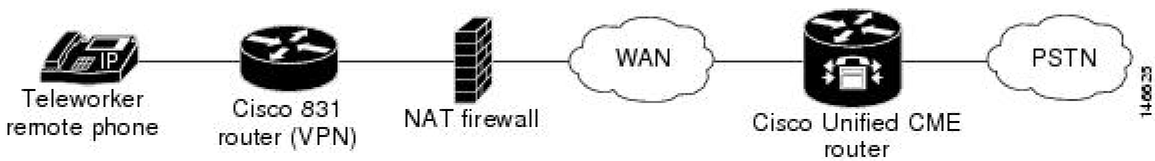
IP phones or a Cisco IP Communicator can be connected to a Cisco Unified CME system over a WAN to support teleworkers who have offices that are remote from the Cisco Unified CME router. The maximum number of remote phones that can be supported is determined by the available bandwidth.

IP addressing is a determining factor in the most critical aspect of remote teleworker phone design. The following two scenarios represent the most common designs, the second one is the most common for small and medium businesses:

- Remote site IP phones and the hub Cisco Unified CME router use globally routable IP addresses.
- Remote site IP phones use NAT with unroutable private IP addresses and the hub Cisco Unified CME router uses a globally routable address (see Figure 13: Remote Site IP Phones Using NAT, on page 245). This scenario results in one-way audio unless you use one of the following workarounds:
    - Configure static NAT mapping on the remote site router (for example, a Cisco 831 Ethernet Broadband Router) to convert between a private address and a globally routable address. This solution uses fewer Cisco Unified CME resources, but voice is unencryped across the WAN.
    - Configure an IPsec VPN tunnel between the remote site router (For example, a Cisco 831 Ethernet Broadband Router) and the Cisco Unified CME router. This solution requires Advanced IP Services

or higher image on the Cisco Unified CME router if this router is used to terminate the VPN tunnel. Voice will be encrypted across the WAN. This method will also work with the Cisco VPN client on a PC to support a Cisco IP Communicator.

Figure 13: Remote Site IP Phones Using NAT



Media Termination Point for Remote Phones

Media termination point (MTP) configuration is used to ensure that Real-Time Transport Protocol (RTP) media packets from remote phones always transit through the Cisco Unified CME router. Without the MTP feature, a phone that is connected in a call with another phone in the same Cisco Unified CME system sends its media packets directly to the other phone, without the packets going through the Cisco Unified CME router. MTP forces the packets to be sourced from the Cisco Unified CME router.

When this configuration is used to instruct a phone to always send its media packets to the Cisco Unified CME router, the router acts as an MTP or proxy and forwards the packets to the destination phone. If a firewall is present, it can be configured to pass the RTP packets because the router uses a specified UDP port for media packets. In this way, RTP packets from remote IP phones can be delivered to IP phones on the same system though they must pass through a firewall.

You must use the **mtp** command to explicitly enable MTP for each remote phone that sends media packets to Cisco Unified CME.

One factor to consider is whether you are using multicast music on hold (MOH) in your system. Multicast packets generally cannot be forwarded to phones that are reached over a WAN. The multicast MOH feature checks to see if MTP is enabled for a phone and if it is, MOH is not sent to that phone. If you have a WAN configuration that can forward multicast packets and you can allow RTP packets through your firewall, you can decide not to use MTP.

For configuration information, see Enable Remote Phone, on page 307.

G.729r8 Codec on Remote Phones

You can select the G.729r8 codec on a remote IP phone to help save network bandwidth. The default codec is G.711 mu-law. If you use the **codec g729r8** command without the **dspfarm-assist** keyword, the use of the G.729 codec is preserved only for calls between two phones on the Cisco Unified CME router (such as between an IP phone and another IP phone or between an IP phone and an FXS analog phone). The **codec g729r8** command has no effect on a call directed through a VoIP dial peer unless the **dspfarm-assist** keyword is also used.

For configuration information, see Enable Remote Phone, on page 307.

For information about transcoding behavior when using the G.729r8 codec, see Transcoding When a Remote Phone Uses G.729r8, on page 478.

Busy Trigger and Channel Huntstop for SIP Phones

Cisco Unified CME 7.1 introduced busy trigger and huntstop channel support for SIP phones, such as the Cisco Unified IP Phone 7941G, 7941GE, 7942G, 7945G, 7961G, 7961GE, 7962G, 7965G, 7970G, 7971GE, 7975G, and 7985. For these SIP phones, the number of channels supported is limited by the amount of memory on the phone. To prevent incoming calls from overloading the phone, you can configure a busy trigger and a channel huntstop for the directory numbers on the phone.

The Channel Huntstop feature limits the number of channels available for incoming calls to a directory number. If the number of incoming calls reaches the configured limit, Cisco Unified CME does not present the next incoming call to the directory number. This reserves the remaining channels for outgoing calls or for features, such as call transfer and conferencing.

The Busy Trigger feature limits the calls to a directory number by triggering a busy response. After the number of active calls, both incoming and outgoing, reaches the configured limit, Cisco Unified CME forwards the next incoming call to the Call Forward Busy destination or rejects the call with a busy tone if Call Forward Busy is not configured.

The busy-trigger limit applies to all directory numbers on a phone. If a directory number is shared among multiple SIP phones, Cisco Unified CME presents incoming calls to those phones that have not reached their busy-trigger limit. Cisco Unified CME initiates the busy trigger for an incoming call only if all the phones sharing the directory number exceed their limit.

For configuration information, see Create Directory Numbers for SIP Phones, on page 263 and Assign Directory Numbers to SIP Phones, on page 266.

Multiple Calls Per Line

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

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

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

In Cisco Unified CME 9.0, the MCPL feature is not supported on Cisco Unified 6921, 6941, 6945, and 6961 SCCP IP phones.

Cisco Unified 8941 and 8945 SCCP IP Phones

Before Cisco Unified CME 9.0, Cisco Unified 8941 and 8945 SCCP IP phones only supported two incoming calls per line and a third channel was reserved for call transfers or conference calls. These phones were also hardcoded with **ephone-dn octo-line**, **huntstop-channel** 2,**max-calls -per-button** 3, and **busy-trigger-per-button** 2.

In Cisco Unified CME 9.0, you can configure the **ephone-dn dn-tag** [**dual-line** | **octo-line**] in global configuration mode and the **max-calls-per-button** and **busy-trigger-per-button** commands in ephone or ephone-template configuration mode for Cisco Unified 8941 and 8945 SCCP IP phones to configure a DN and enable the number of calls per DN, set the maximum number of calls allowed on an octo-line DN, and set the maximum number of calls allowed on an octo-line DN before activating a busy tone.

For configuration information, see Configure the Maximum Number of Calls on SCCP Phone, on page 319.

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

In Cisco Unified CME 9.0, the default values for the **busy-trigger-per-button** command is 1 for the Cisco Unified 6921, 6941, 6945, and 6961 SIP IP phones and 2 for the Cisco Unified 8941 and 8945 SIP IP phones.

You can configure the maximum number of calls before a phone receives a busy tone. For example, if you configure **busy-trigger-per-button** 2 in voice register pool configuration mode for a Cisco Unified 6921, 6941, 6945, or 6961 SIP IP phone, the third incoming call to the phone receives a busy tone.

For information on the Busy Trigger feature on Cisco Unified SIP IP phones, see Busy Trigger and Channel Huntstop for SIP Phones, on page 246.

For configuration information, see Configure the Busy Trigger Limit on SIP Phone, on page 322.

Digit Collection on SIP Phones

Digit strings dialed by phone users must be collected and matched against predefined patterns to place calls to the destination corresponding to the user's input. Before Cisco Unified CME 4.1, SIP phone users had to press the DIAL softkey or # key or wait for the interdigit-timeout to trigger call processing. In Cisco Unified CME 4.1 and later versions, two methods of collecting and matching digits are supported for SIP phones, depending on the model of phone:

Key Press Markup Language Digit Collection

Key Press Markup Language (KPML) uses SIP SUBSCRIBE and NOTIFY methods to report user input digit by digit. Each digit dialed by the phone user generates its own signaling message to Cisco Unified CME, which performs pattern recognition by matching a destination pattern to a dial peer as it collects the dialed digits. This process of relaying each digit immediately is similar to the process used by SCCP phones. It eliminates the need for the user to press the Dial softkey or wait for the interdigit timeout before the digits are sent to Cisco Unified CME for processing.

KPML is supported on Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE. For configuration information, see Enable KPML on a SIP Phone, on page 273.

SIP Dial Plans

A dial plan is a set of dial patterns that SIP phones use to determine when digit collection is complete after a user goes off-hook and dials a destination number. Dial plans allow SIP phones to perform local digit collection and recognize dial patterns as user input is collected. After a pattern is recognized, the SIP phone sends an INVITE message to Cisco Unified CME to initiate the call to the number matching the user's input. All of the digits entered by the user are presented as a block to Cisco Unified CME for processing. Because digit collection is done by the phone, dial plans reduce signaling messages overhead compared to KPML digit collection.

SIP dial plans eliminate the need for a user to press the Dial softkey or # key or to wait for the interdigit timeout to trigger an outgoing INVITE. You configure a SIP dial plan and associate the dial plan with a SIP phone. The dial plan is downloaded to the phone in the configuration file.

You can configure SIP dial plans and associate them with the following SIP phones:

- Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE—These phones use dial plans and support KPML. If both a dial plan and KPML are enabled, the dial plan has priority.

If a matching dial plan is not found and KPML is disabled, the user must wait for the interdigit timeout before the SIP NOTIFY message is sent to Cisco Unified CME. Unlike other SIP phones, these phones do not have a Dial softkey to indicate the end of dialing, except when on-hook dialing is used. In this case, the user can press the Dial softkey at any time to send all the dialed digits to Cisco Unified CME.

- Cisco Unified IP Phones 7905, 7912, 7940, and 7960—These phones use dial plans and do not support KPML. If you do not configure a SIP dial plan for these phones, or if the dialed digits do not match a dial plan, the user must press the Dial softkey or wait for the interdigit timeout before digits are sent to Cisco Unified CME.

When you reset a phone, the phone requests its configuration files from the TFTP server, which builds the appropriate configuration files depending on the type of phone.

- Cisco Unified IP Phones 7905 and 7912—The dial plan is a field in their configuration files.
- Cisco Unified IP Phones 7911G, 7940, 7941G, 7941GE, 7960, 7961G, 7961GE, 7970G, and 7971GE—The dial plan is a separate XML file that is pointed to from the normal configuration file.

For configuration information for Cisco Unified CME, see Configure Dial Plans for SIP Phones, on page 269.

Session Transport Protocol for SIP Phones

In Cisco Unified CME 4.1 and later versions, you can select TCP as the transport protocol for connecting supported SIP phones to Cisco Unified CME. Previously only UDP was supported. TCP is selected for individual SIP phones by using the **session-transport** command in voice register pool or voice register template configuration mode. For configuration information, see Select Session-Transport Protocol for a SIP Phone, on page 275.

Real-Time Transport Protocol Call Information Display Enhancement

Before Cisco Unified CME 8.8, active RTP call information on ephone call legs were determined only by parsing the **show ephone registered** or **show ephone offhook** command output. The **show voip rtp connections** command showed active call information in the system but it did not apply to ephone call legs. In Cisco Unified CME 8.8 and later versions, you can display information on active RTP calls, including the ephone tag number of the phone with an active call, the channel of the ephone-dn, and the caller and called party's numbers for the connection for both local and remote endpoints, using the **show ephone rtp connections** command. The output from this command provides an overview of all the connections in the system, narrowing the criteria for debugging pulse code modulation and Cisco Unified CME packets without a sniffer.

Note When an ephone to non-ephone call is made, information on the non-ephone does not appear in a **show ephone rtp connections** command output. To display the non-ephone call information, use the **show voip rtp connections** command.

The following sample output shows all the connected ephones in the Cisco Unified CME system. The sample output shows five active ephone connections with one of the phones having the **dspfarm-assist** keyword configured to transcode the code on the local leg to the indicated codec. The output also shows four ephone-to-ephone calls, represented in the CallID columns of both the RTP connection source and RTP connection destination by zero values.

Normally, a phone can have only one active connection but in the presence of a whisper intercom call, a phone can have two. In the sample output, ephone-40 has two active calls: it is receiving both a normal call and a whisper intercom call. The whisper intercom call is being sent by ephone-6, which has an invalid LocalIP of 0.0.0.0. The invalid LocalIP indicates that it does not receive RTP audio because it only has a one-way voice connection to the whisper intercom call recipient.

```
Router# show ephone rtp connections
Ephone RTP active connections :
Ephone     Line  DN Chan  SrcCallID  DstCallID Codec (xcoded?)
    SrcNum DstNum  LocalIP             RemoteIP
ephone-5     1   5    1         15         14 G729 (Y)
    1005  1102  [192.168.1.100]:23192  [192.168.1.1]:2000
ephone-6     2  35    1          0          0       G711Ulaw64k (N)
    1035  1036  [0.0.0.0]:0  [192.168.1.81]:21256
ephone-40    1 140    1          0          0       G711Ulaw64k (N)
    1140  1141  [192.168.1.81]:21244  [192.168.1.70]:20664
ephone-40    2  36    1          0          0       G711Ulaw64k (N)
    1035  1036  [192.168.1.81]:21256  [192.168.1.1]:2000
ephone-41    1 141    1          0          0       G711Ulaw64k (N)
    1140  1141  [192.168.1.70]:20664  [192.168.1.81]:21244
Found 5 active ephone RTP connections
```

Ephone-Type Configuration

In Cisco Unified CME 4.3 and later versions, you can dynamically add a new phone type to your configuration without upgrading your Cisco IOS software. New phone models that do not introduce new features can easily be added to your configuration without requiring a software upgrade.

The ephone-type configuration template is a set of commands that describe the features supported by a type of phone, such as the particular phone type's device ID, number of buttons, and security support. Other phone-related settings under telephony-service, ephone-template, and ephone configuration mode can override the features set within the ephone-type template. For example, an ephone-type template can specify that a particular phone type supports security and another configuration setting can disable this feature. However, if an ephone-type template specifies that this phone does not support security, the other configuration cannot enable support for the security feature.

Cisco Unified CME uses the ephone-type template to generate XML files to provision the phone. System-defined phone types continue to be supported without using the ephone-type configuration. Cisco Unified CME checks the ephone-type against the system-defined phone types. If there is conflict with the phone type or the device ID, the configuration is rejected.

For configuration information, see Configure Ephone-Type Templates for SCCP Phones, on page 256.

7926G Wireless SCCP IP Phone Support

Cisco Unified CME 8.6 adds support for the Cisco Unified 7926G Wireless SCCP IP phone. The 7926G wireless phone is phone similar to the 7925 wireless phone with a 2D barcode and EA15 module attached. The 7926G wireless phone is capable of scanning functionality. For more details on phone features and functionality, see Cisco Unified IP Phone 7900 Series User Guide.

Cisco Unified CME 8.6 supports the scanning function on the 7926G SCCP wireless phone using the ephone built-in device type. Table 16: Supported Values for Ephone-Type Command , on page 250 shows supported values for the ephone-type for 7926G wireless phone.

Table 16: Supported Values for Ephone-Type Command

Supported Device	device-id	device-type	num-buttons	max-presentation
Cisco Unified Wireless IP Phone 7926G	577	7926	6	2

To support service provisioning, an XML file is constructed externally and applied to the ephone-template of the phone. To allow the phone to read the external XML file, you are required to create-cnf and download the XML file to the ephone. For more information on configuring PhoneServices XML file, see Configure Phone Services XML File for Cisco Unified Wireless Phone 7926G, on page 313.

The following is an example of the <phoneServices> XML file:

```
<phoneServices  useHTTPS="true">
<provisioning>0</provisioning>
<phoneService  type="1" category="0">
<name>Missed Calls</name>
<url>Application:Cisco/MissedCalls</url>
<vendor></vendor>
<version></version>
</phoneService>
<phoneService  type="0" category="1">
<displayName>Store Ops</displayName>
<name>Store Ops</name>
<url>http://1.4.206.105/Midlets/StoreOps.jad?StoreNumber=1777</url>
<http://1.4.206.105/Midlets/StoreOps.jad?StoreNumber=1777%3c/url%3e>
<http://1.4.206.105/Midlets/StoreOps.jad?StoreNumber=1777%3c/url%3e>
<vendor>CiscoSystems</vendor>
<version>0.0.82</version>
</phoneService>
</phoneServices>
```

KEM Support for Cisco Unified SIP IP Phones

For information on the KEM support for Cisco Unified 8851/51NR, 8861, 8961, 9951, and 9971 SIP IP Phones, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Key Mapping

The mapping of configured keys on a phone depends on the number of KEMs attached to the phone.

If only one KEM is attached to a phone and the number of keys configured is 114, only 36 keys on the KEM are mapped to the configured keys on the phone. The rest of the keys are not visible on the phone or the KEM.

Call Control

All call control features are supported by KEMs on Cisco Unified 8961 SIP IP phones. Any feature that can be configured on the phone keys can also be configured on the KEM.

Because the Transfer, Hold, and Conference keys are built-in keys on Cisco Unified 8851/51NR, 8861, 8961, 9951 and 9971 SIP IP Phones, these features cannot be mapped to the keys on the KEMs.

XML Updates

- There is no separate firmware for KEMs, instead they are built in as part of the phones.
- The number of XML entries in the configuration file increases with the number of keys configured.
- The device type for KEMs is CKEM and the maximum number of supported keys on each KEM device is 36.

Restrictions for KEM Support

- KEMs are not supported for Cisco Unified SCCP IP phones and Cisco Unified SIP IP phones other than the Cisco Unified 8851/51NR, 8861, 8961, 9951, and 9971 SIP IP phones.
- Features configured on keys are disabled when supported Cisco Unified SIP IP phones are in Cisco Unified SIP SRST.
- All Cisco Unified 8851/51NR, 8861, 8961, 9951, and 9971 SIP IP phone restrictions and limitations apply to KEMs.
- All Cisco Unified CME and Cisco Unified SIP SRST feature restrictions and limitations apply to KEMs.

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

For information on installing KEMs on Cisco Unified IP Phone, see "*Installing a Key Expansion Module on the Cisco Unified IP Phone*" section of Cisco Unified IP Phone 8961, 9951, and 9971 Administration Guide for Cisco Unified Communications Manager 10.0 .

For information on installing KEMs on Cisco Unified 8811, 8841, 8851, 8851NR, and 8861 Phones, see *Cisco IP Phone Key Expansion Module* section of Cisco IP Phone 8800 Series Administration Guide for Cisco Unified Communications Manager.

Fast-Track Configuration Approach for Cisco Unified SIP IP Phones

In Cisco Unified CME Release 10.0, the Fast-Track Configuration feature provides a new configuration utility using which you can input the phone characteristics of a new SIP phone model. This utility allows you to configure the existing SIP line features to the new SIP phone models. In the fast-track configuration, an option is provided to input an existing SIP phone as a reference phone. This feature is supported only on new SIP phone models that do not need any changes in the software protocols and the Cisco Unified CME application.

Note To deploy Cisco Unified SIP IP phones on Cisco Unified CME using the fast-track configuration approach, you require Cisco IOS Release 15.3(3)M or a later release.

Forward Compatibility

When a new SIP phone model is configured using the fast-track configuration approach. and the Cisco Unified CME is upgraded to a later version that supports the new SIP phone model, the fast-track configuration pertaining to that SIP phone model is removed automatically. If the Cisco Unified CME is downgraded to a version that does not have the built-in support, the fast-track configuration should be applied again.

To support Fast-Track Configuration feature, the **voice register pool-type** command has been introduced in the global configuration mode. The properties of the new SIP phone can be configured under the voice register pool-type submode. In addition to the explicit configuration of the phone's properties, the reference-pooltype option can be used to inherit the properties of an existing SIP phone.

Localization support

CME supports localization for phones in fast-track mode through locale installer. However, the locale package should have .jar files for a specific phone model to make the feature work.

To use the locale installer, see Locale Installer for Cisco Unified SIP IP Phones, on page 411 .

For new SIP phone models validated using Fast-track configuration and the supported locale package version, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Restrictions for Fast-Track Support

- The fast-track configuration does not allow you to use the following phone models as reference phone:
  - ATA—Cisco ATA-186 and Cisco ATA-188
  - 7905—Cisco Unified IP Phone 7905 and Cisco Unified IP Phone 7905G
  - 7912—Cisco Unified IP Phone 7912 and Cisco Unified IP Phone 7912G
  - 7940—Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7940G
  - 7960—Cisco Unified IP Phone 7960 and Cisco Unified IP Phone 7960G
  - P100—PingTel Xpressa 100
  - P600—Polycom SoundPoint IP 600
  - Existing Cisco Unified SIP IP phones are not allowed to be configured as new Cisco Unified SIP IP phones using the fast-track configuration approach.
  - The reference-pooltype functionality is allowed only on existing SIP phone models. New SIP phone models configured using the fast-track configuration approach cannot be used as a reference phone.
  - The fast-track configuration approach supports only the XML format and not support the text format for phone configuration.
  - The fast-track approach does not support the new SIP phone models that have a new call flow, new message flow, or a new configuration file format that are not supported by the Cisco Unified CME.

For configuration information, see Provision SIP Phones to Use the Fast-Track Configuration Approach, on page 325.

For configuration examples, see Example for Fast-Track Configuration Approach, on page 340.

Configure Phones for a PBX System

This section contains the following tasks:

Create Directory Numbers for SCCP Phones

To create a directory number in Cisco Unified CME for a SCCP phone, intercom line, voice port, or a message-waiting indicator (MWI), perform the following steps for each directory number to be created. Each ephone-dn becomes a virtual line, or extension, on which call connections can be made. Each ephone-dn configuration automatically creates one or more virtual dial peers and virtual voice ports to make those call connections.

Note To create and assign directory numbers to be included in an overlay set, see Configure Overlaid Ephone-dns on SCCP Phones, on page 1326.

Restriction

- The Cisco Unified IP Phone 7931G is a SCCP keyset phone and, when configured for a key system, does not support the dual-line option for a directory number. To configure a Cisco Unified IP Phone 7931G, see Configure Phones for a Key System, on page 282.
- Octo-line directory numbers are not supported by the Cisco Unified IP Phone 7902, 7920, or 7931, or by analog phones connected to the Cisco VG224 or Cisco ATA.
- Octo-line directory numbers are not supported in button overlay sets.
- Octo-line directory numbers do not support the **trunk** command.

Before You Begin

- Maximum number of directory numbers must be changed from the default of 0 by using the **max-dn** command.
- Octo-line directory numbers are supported in Cisco Unified CME 4.3 and later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line** | **octo-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **huntstop** [**channel** *number*]
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	**ephone-dn** *dn-tag* [**dual-line** | **octo-line**] **Example:** `Router(config)# ephone-dn 7 octo-line`	Enters ephone-dn configuration mode to create a directory number for a SCCP phone. • **dual-line**—(Optional) Enables two calls per directory number. Supports features such as call waiting, call transfer, and conferencing with a single ephone-dn. • **octo-line**—(Optional) Enables eight calls per directory number. Supported in Cisco Unified CME 4.3 and later versions. • To change the line mode of a directory number, for example from dual-line to octo-line or the reverse, you must first delete the ephone-dn and then recreate it.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 2001`	Configures an extension number for this directory number. • Configuring a secondary number supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.
Step 5	**huntstop** [**channel** *number*] **Example:** `Router(config-ephone-dn)# huntstop channel 4`	(Optional) Enables Channel Huntstop, which keeps a call from hunting to the next channel of a directory number if the first channel is busy or does not answer. • **channel** *number*—Number of channels available to accept incoming calls. Remaining channels are reserved for outgoing calls and features such as call transfer, call waiting, and conferencing. Range: 1 to 8. Default: 8. • *number* argument is supported for octo-line directory numbers only.
Step 6	**name** *name* **Example:** `Router(config-ephone-dn)# name Smith, John`	(Optional) Associates a name with this directory number. • Name is used for caller-ID displays and in the local directory listings. • Must follow the name order that is specified with the **directory** command.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Example for Nonshared Octo-Line Directory Number

In the following example, ephone-dn 7 is assigned to phone 10 and not shared by any other phone. There are two active calls on ephone-dn 7. Because the **busy-trigger-per-button** command is set to 2, a third incoming call to extension 2001 is either rejected with a busy tone or forwarded to another destination if Call Forward Busy is configured. The phone user can still make an outgoing call or transfer or conference a call on ephone-dn 7 because the **max-calls-per-button** command is set to 3, which allows a total of three calls on ephone-dn 7.

```
ephone-dn  7  octo-line
 number 2001
 name Smith, John
 huntstop channel 4
!
!
ephone  10
 max-calls-per-button 3
 busy-trigger-per-button 2
 mac-address 00E1.CB13.0395
 type 7960
 button  1:7
```

Example for Shared Octo-Line Directory Number

In the following example, ephone-dn 7 is shared between phone 10 and phone 11. There are two active calls on ephone-dn 7. A third incoming call to ephone-dn 7 rings only phone 11 because its **busy-trigger-per-button** command is set to 3. Phone 10 allows a total of three calls, but it rejects the third incoming call because its **busy-trigger-per-button** command is set to 2. A fourth incoming call to ephone-dn 7 on ephone 11 is either rejected with a busy tone or forwarded to another destination if Call Forward Busy is configured. The phone user can still make an outgoing call or transfer or conference a call on ephone-dn 7 on phone 11 because the **max-calls-per-button** command is set to 4, which allows a total of four calls on ephone-dn 7 on phone 11.

```
ephone-dn  7  octo-line
 number 2001
 name Smith, John
 huntstop channel 4
!
!
ephone  10
 max-calls-per-button 3
 busy-trigger-per-button 2
 mac-address 00E1.CB13.0395>
 type 7960
 button  1:7
!
!
!
ephone  11
 max-calls-per-button 4
 busy-trigger-per-button 3
 mac-address 0016.9DEF.1A70
 type 7960
 button  1:7
```

What to Do Next

After creating directory numbers, you can assign one or more directory numbers to a Cisco Unified IP Phone. See Assign Directory Numbers to SCCP Phones, on page 260.

Configure Ephone-Type Templates for SCCP Phones

Restriction	Ephone-type templates are not supported for system-defined phone types. For a list of system-defined phone types, see the **type** command in Cisco Unified CME Command Reference.

Before You Begin

Cisco Unified CME 4.3 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-type** *phone-type* [**addon**]
4. **device-id** *number*
5. **device-name** *name*
6. **device-type** *phone-type*
7. **num-buttons** *number*
8. **max-presentation** *number*
9. **addon**
10. **security**
11. **phoneload**
12. **utf8**
13. **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.

	Command or Action	Purpose
Step 3	**ephone-type** *phone-type* [**addon**] **Example:** `Router(config)# ephone-type E61`	Enters ephone-type configuration mode to create an ephone-type template. • *phone-type*—Unique label that identifies the type of IP phone for which the phone-type template is being defined. • **addon**—(Optional) Phone type is an add-on module, such as the Cisco Unified IP Phone 7915 Expansion Module.
Step 4	**device-id** *number* **Example:** `Router(config-ephone-type)# device-id 376`	Specifies the device ID for the phone type. • This device ID must match the predefined device ID for the specific phone model. • If this command is set to the default value of 0, the ephone-type is invalid. • See Table 17: Supported Values for Ephone-Type Commands , on page 258 for a list of supported device IDs.
Step 5	**device-name** *name* **Example:** `Router(config-ephone-type)# device-name E61 Mobile Phone`	Assigns a name to the phone type. • See Table 17: Supported Values for Ephone-Type Commands , on page 258 for a list of supported device types.
Step 6	**device-type** *phone-type* **Example:** `Router(config-ephone-type)# device-type E61`	Specifies the device type for the phone.
Step 7	**num-buttons** *number* **Example:** `Router(config-ephone-type)# num-buttons 1`	Number of line buttons supported by the phone type. • *number*—Range: 1 to 100. Default: 0. • See Table 17: Supported Values for Ephone-Type Commands , on page 258 for the number of buttons supported by each phone type.
Step 8	**max-presentation** *number* **Example:** `Router(config-ephone-type)# max-presentation 1`	Number of call presentation lines supported by the phone type. • *number*—Range: 1 to 100. Default: 0. • See Table 17: Supported Values for Ephone-Type Commands , on page 258 for the number of presentation lines supported by each phone type.
Step 9	**addon** **Example:** `Router(config-ephone-type)# addon`	(Optional) Specifies that this phone type supports an add-on module, such as the Cisco Unified IP Phone 7915 Expansion Module.

	Command or Action	Purpose
Step 10	**security** **Example:** `Router(config-ephone-type)# security`	(Optional) Specifies that this phone type supports security features. • This command is enabled by default.
Step 11	**phoneload** **Example:** `Router(config-ephone-type)# phoneload`	(Optional) Specifies that this phone type requires that the **load** command be configured. • This command is enabled by default.
Step 12	**utf8** **Example:** `Router(config-ephone-type)# utf8`	(Optional) Specifies that this phone type supports UTF8. • This command is enabled by default.
Step 13	**end** **Example:** `Router(config-ephone-type)# end`	Exits to privileged EXEC mode.

Ephone-Type Parameters for Supported Phone Types

Table 17: Supported Values for Ephone-Type Commands , on page 258 lists the required device ID, device type, and the maximum number of buttons and call presentation lines that are supported for each phone type that can be added with ephone-type templates.

Table 17: Supported Values for Ephone-Type Commands

Supported Device	device-id	device-type	num-buttons	max-presentation
Cisco Unified IP Phoone 6901	547	6901	1	1
Cisco Unified IP Phone 6911	548	6911	10	1
Cisco Unified IP Phone 6945	564	6945	4	2
Cisco Unified IP Phone 7915 Expansion Module with 12 buttons	227	7915	12	0 (default)

Supported Device	device-id	device-type	num-buttons	max-presentation
Cisco Unified IP Phone 7915 Expansion Module with 24 buttons	228	7915	24	0
Cisco Unified IP Phone 7916 Expansion Module with 12 buttons	229	7916	12	0
Cisco Unified IP Phone 7916 Expansion Module with 24 buttons	230	7916	24	0
Cisco Unified Wireless IP Phone 7925	484	7925	6	4
Cisco Unified IP Conference Station 7937G	431	7937	1	6
Cisco Unified IP Phone 8941	586	8941	4	3
Cisco Unified IP Phone 8945	585	8945	4	3
Cisco Unified IP Phone 8941 with Fast-Track configuration support	586	8941	4	3
Cisco Unified IP Phone 8945 with Fast-Track configuration support	586	8945	4	3
Nokia E61	376	E61	1	1

Example

The following example shows the Nokia E61 added with an ephone-type template, which is then assigned to ephone 2:

```
ephone-type  E61
 device-id 376
 device-name E61 Mobile Phone
 num-buttons 1
 max-presentation 1
 no utf8
 no phoneload
!
ephone  2
 mac-address 001C.821C.ED23
 type E61
 button  1:2
```

Assign Directory Numbers to SCCP Phones

This task sets up the initial ephone-dn-to-ephone relationships: how and which extensions appear on each phone. To create and modify phone-specific parameters for individual SCCP phones, perform the following steps for each SCCP phone to be connected in Cisco Unified CME. While using the GUI to administer ephone-dns on CME, ensure ephone-dns value is lower than the max-dns value.

Note

To create and assign directory numbers to be included in an overlay set, see Configure Overlaid Ephone-dns on SCCP Phones, on page 1326.

Restriction

- For Watch mode. If the watched directory number is associated with several phones, then the watched phone is the one on which the watched directory number is on button 1 or the one on which the watched directory number is on the button that is configured by using the**auto-line** command, with auto-line having priority. For configuration information, see Automatic Line Selection, on page 1041.
- Octo-line directory numbers are not supported by the Cisco Unified IP Phone 7902, 7920, or 7931, or by analog phones connected to the Cisco VG224 or Cisco ATA.
- Octo-line directory numbers are not supported in button overlay sets.

Before You Begin

- To configure a phone line for Watch (w) mode by using the **button** command, Cisco Unified CME 4.1 or a later version.
- To configure a phone line for Monitor (m) mode by using the **button** command, Cisco CME 3.0 or a later version.
- To assign a user-defined phone type in Cisco Unified CME 4.3 or a later version, you must first create an ephone-type template. See Configure Ephone-Type Templates for SCCP Phones, on page 256.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mac-address** [*mac-address*]
5. **type** *phone-type* [**addon 1** *module-type* [**2** *module-type*]]
6. **button** *button-number* {*separator*}*dn-tag* [**,** *dn-tag...*] [*button-number* {**x**} *overlay-button-number*] [*button-number...*]
7. **max-calls-per-button** *number*
8. **busy-trigger-per-button** *number*
9. **keypad-normalize**
10. **nte-end-digit-delay** [*milliseconds*]
11. **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** *phone-tag* **Example:** `Router(config)#ephone 6`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type **?** to display range.
Step 4	**mac-address** [*mac-address*] **Example:** `Router(config-ephone)#mac-address 2946.3f2.311`	Specifies the MAC address of the IP phone that is being configured. • *mac-address*—(Optional) For CiscoUnifiedCME 3.0 and later versions, it is not required to register phones before configuring the phone because CiscoUnifiedCME can detect MAC addresses and automatically populate phone configurations with the MAC addresses and phone types for individual phones. Not supported for voice-mail ports.
Step 5	**type** *phone-type* [**addon 1** *module-type* [**2** *module-type*]]	Specifies the type of phone. • CiscoUnifiedCME 4.0 and later versionsThe only types to which you can apply an add-on module are **7960**, **7961**,**7961GE**, and **7970**.

	Command or Action	Purpose
	Example: `Router(config-ephone)# type 7960 addon 1 7914`	• CiscoCME 3.4 and earlier versionsThe only type to which you can apply an add-on module is **7960**.
Step 6	**button** *button-number* {*separator*}*dn-tag* [**,** *dn-tag...*] [*button-number* {**x**} *overlay-button-number*] [*button-number...*] **Example:** `Router(config-ephone)# button 1:10 2:11 3b12 4o13,14,15`	Associates a button number and line characteristics with an extension (ephone-dn). Maximum number of buttons is determined by phone type. **Note** The CiscoUnified IPPhone7910 has only one line button but can be given two ephone-dn tags.
Step 7	**max-calls-per-button** *number* **Example:** `Router(config-ephone)# max-calls-per-button 3`	(Optional) Sets the maximum number of calls, incoming and outgoing, allowed on an octo-line directory number on this phone. • *number*—Range: 1 to 8. Default: 8. • This command is supported in CiscoUnifiedCME4.3 and later versions. • This command must be set to a value that is more than or equal to the value set with the busy-trigger-per-button command. • This command can also be configured in ephone-template configuration mode and applied to one or more phones. The ephone configuration has priority over the ephone-template configuration.
Step 8	**busy-trigger-per-button** *number* **Example:** `Router(config-ephone)# busy-trigger-per-button 2`	(Optional) Sets the maximum number of calls allowed on this phones octo-line directory numbers before triggering Call Forward Busy or a busy tone. • *number*—Range: 1 to 8. Default: 0 (disabled). • This command is supported in CiscoUnifiedCME4.3 and later versions. • After the number of existing calls, incoming and outgoing, on an octo-line directory number exceeds the number of calls set with this command, the next incoming call to the directory number is forwarded to the Call Forward Busy destination if configured, or the call is rejected with a busy tone. • This command must be set to a value that is less than or equal to the value set with the **max-calls-per-button** command. • This command can also be configured in ephone-template configuration mode and applied to one or more phones. The ephone configuration has priority over the ephone-template configuration.
Step 9	**keypad-normalize** **Example:** `Router(config-ephone)# keypad-normalize`	(Optional) Imposes a 200-millisecond delay before each keypad message from an IP phone. • When used with the **nte-end-digit-delay** command, this command ensures that the delay configured for a dtmf-end event is always honored.

	Command or Action	Purpose
Step 10	**nte-end-digit-delay** [*milliseconds*] **Example:** `Router(config-ephone)# nte-end-digit-delay 150`	(Optional) Specifies the amount of time that each digit in the RTP NTE end event in an RFC2833 packet is delayed before being sent. • This command is supported in CiscoUnifiedCME 4.3 and later versions. • *milliseconds*—length of delay. Range: 10 to 200. Default: 200. • To enable the delay, you must also configure the **dtmf-interworking rtp-nte** command in voice-service or dial-peer configuration mode. For information, see Enable DTMF Integration Using RFC 2833, on page 562. • This command can also be configured in ephone-template configuration mode. The value set in ephone configuration mode has priority over the value set in ephone-template mode.
Step 11	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Example for assigning directory number to SCCP Phone

The following example assigns extension 2225 in the Accounting Department to button 1 on ephone 2:

```
ephone-dn 25
 number 2225
 name Accounting

 ephone 2
 mac-address 00E1.CB13.0395
 type 7960
 button 1:25
```

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- After configuring phones in Cisco Unified CME to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Create Directory Numbers for SIP Phones

To create a directory number in Cisco Unified CME for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI), perform the following steps for each directory number to be created.

Restriction

- Valid characters in voice register dn include 0-9, '.', '+', '*', and '#'.
- To allow insertion of '#' at any place in voice register dn, the CLI "allow-hash-in-dn" is configured in voice register global mode.
- When the CLI "allow-hash-in-dn" is configured, the user is required to change the dial-peer terminator from '#' (default terminator) to another valid terminator in configuration mode. The other terminators that are supported include '0'-'9', 'A'-'F', and '*'.
- Maximum number of directory numbers supported by a router is version and platform dependent.
- Call Forward All, Presence, and message-waiting indication (MWI) features in Cisco Unified CME 4.1 and later versions require that SIP phones be configured with a directory number using the **dn** keyword with the **number** command; direct line numbers are not supported.
- SIP endpoints are not supported on H.323 trunks. SIP endpoints are supported on SIP trunks only.
- The Media Flow-around feature configured with the **media flow-around** command is not supported by Cisco Unified CME with SIP phones.
- SIP shared-line directory numbers are not supported by the Cisco Unified IP Phone 7902, 7920, 7931, 7940, or 7960, or by analog phones connected to the Cisco VG224 or Cisco ATA.
- For Unified CME 12.1 and prior releases, SIP shared-line directory numbers cannot be members of hunt groups.

Before You Begin

- Cisco CME 3.4 or a later version.
- SIP shared-line directory numbers are supported in Cisco Unified CME 7.1 and later versions.
- **registrar server** command must be configured. For configuration information, see Enable Calls in Your VoIP Network, on page 125.
- In Cisco Unified CME 7.1 and later versions, the maximum number of directory numbers must be changed from the default of 0 by using the **max-dn** (voice register global) command. For configuration information, see Set Up Cisco Unified CME for SIP Phones, on page 192.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **shared-line** [**max-calls** *number-of-calls*]
6. **huntstop channel** *number-of-channels*
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 register dn** *dn-tag* **Example:** `Router(config)# voice register dn 17`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI).
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 7001`	Defines a valid number for a directory number.
Step 5	**shared-line** [**max-calls** *number-of-calls*] **Example:** `Router(config-register-dn)# shared-line max-calls 6`	(Optional) Creates a shared-line directory number. • **max-calls** *number-of-calls* (Optional)—Maximum number of calls, both incoming and outgoing. Range: 2 to 16. Default: 2. • Must be set to a value that is more than or equal to the value set with the **busy-trigger-per-button** command. • This command is supported in Cisco Unified CME 7.1 and later versions.
Step 6	**huntstop channel** *number-of-channels* **Example:** `Router(config-register-dn)# huntstop channel 3`	(Optional) Enables Channel Huntstop, which keeps a call from hunting to the next channel of a directory number if the first channel is busy or does not answer. • *number-of-channels*—Number of channels available to accept incoming calls on the directory number. Remaining channels are reserved for outgoing calls and features, such as Call Transfer, Call Waiting, and Conferencing. Range: 1 to 50. Default: 0 (disabled). • This command is supported in Cisco Unified CME 7.1 and later versions.
Step 7	**end** **Example:** `Router(config-register-dn)# end`	Exits to privileged EXEC mode.

Example for assigning directory numbers to SIP Phones

The following example shows directory number 24 configured as a shared line and assigned to phone 124 and phone 125:

```
voice register dn  24
 number 8124
 shared-line max-calls 6
!
voice register pool  124
 id mac 0017.E033.0284
 type 7965
 number 1 dn 24
!
voice register pool  125
 id mac 00E1.CB13.0395
 type 7965
number 1 dn 24
```

Assign Directory Numbers to SIP Phones

This task sets up which extensions appear on each phone. To create and modify phone-specific parameters for individual SIP phones, perform the following steps for each SIP phone to be connected in Cisco Unified CME.

Note If your Cisco Unified CME system supports SCCP and SIP phones, do not connect your SIP phones to your network until after you have verified the configuration profile for the SIP phone.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **id** {**network** *address* **mask** *mask* | **ip** *address* **mask** *mask* | **mac** *address*}
5. **type** *phone-type*
6. **number** *tag* **dn** *dn-tag*
7. **busy-trigger-per-button** *number-of-calls*
8. **username** *username* **password** *password*
9. **dtmf-relay** {[**cisco-rtp**] [**rtp-nte**] [**sip-notify**]}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 4	**id** {**network** *address* **mask** *mask* | **ip** *address* **mask** *mask* | **mac** *address*} **Example:** `Router(config-register-pool)# id mac 0009.A3D4.1234`	Explicitly identifies a locally available individual SIP phone to support a degree of authentication.
Step 5	**type** *phone-type* **Example:** `Router(config-register-pool)#` **type** `7960-7940`	Defines a phone type for the SIP phone being configured.
Step 6	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 17`	Associates a directory number with the SIP phone being configured. • **dn** *dn-tag*—identifies the directory number for this SIP phone as defined by the **voice register dn** command.
Step 7	**busy-trigger-per-button** *number-of-calls* **Example:** `Router(config-register-pool)# busy-trigger-per-button 2`	(Optional) Sets the maximum number of calls allowed on any of this phone□s directory numbers before triggering Call Forward Busy or a busy tone. • *number-of-calls*—Maximum number of calls allowed before Cisco Unified CME forwards the next incoming call to the Call Forward Busy destination, if configured, or rejects the call with a busy tone. Range: 1 to 50. • This command is supported in Cisco Unified CME 7.1 and later versions.

	Command or Action	Purpose
Step 8	**username** *username* **password** *password* **Example:** `Router(config-register-pool)# username smith password 123zyx`	(Optional) Required only if authentication is enabled with the **authenticate** command. Creates an authentication credential. **Note** This command is not for SIP proxy registration. The password will not be encrypted. All lines in a phone will share the same credential. • *username*—identifies a local Cisco Unified IP phone user. Default: Admin.
Step 9	**dtmf-relay** {[**cisco-rtp**] [**rtp-nte**] [**sip-notify**]} **Example:** `Router(config-register-pool)# dtmf-relay rtp-nte`	(Optional) Specifies a list of DTMF relay methods that can be used by the SIP phone to relay DTMF tones. **Note** SIP phones natively support in-band DTMF relay as specified in RFC 2833.
Step 10	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Example for configuring SIP Nonshared Line

In the following example, voice register dn 23 is assigned to phone 123. The fourth incoming call to extension 8123 is not presented to the phone because the **huntstop channel** command is set to 3. Because the **busy-trigger-per-button** command is set to 2 on phone 123 and Call Forward Busy is configured, the third incoming call to extension 8123 is forwarded to extension 8200.

```
voice register dn  23
 number 8123
 call-forward b2bua busy 8200
 huntstop channel 3
!
voice register pool  123
 busy-trigger-per-button 2
 id mac 0009.A3D4.1234
 type 7965
 number 1 dn 23
```

Example for configuring SIP Shared Line

In the following example, voice register dn 24 is shared by phones 124 and 125. The first two incoming calls to extension 8124 ring both phones. A third incoming call rings only phone 125 because its **busy-trigger-per-button** command is set to 3. The fourth incoming call to extension 8124 triggers Call Forward Busy because the busy trigger limit on all phones is exceeded.

```
voice register dn  24
 number 8124
 call-forward b2bua busy 8200
 shared-line max-calls 6
 huntstop channel 6
```

```
!
voice register pool  124
 busy-trigger-per-button 2
 id mac 0017.E033.0284
 type 7965
 number 1 dn 24
!
voice register pool  125
 busy-trigger-per-button 3
 id mac 00E1.CB13.0395
 type 7965
 number 1 dn 24
```

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- If you want to select the session-transport protocol for a SIP phone, see Select Session-Transport Protocol for a SIP Phone, on page 275.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Profiles for SIP Phones, on page 391.

Configure Dial Plans for SIP Phones

Dial plans enable SIP phones to recognize digit strings dialed by users. After the phone recognizes a dial pattern, it automatically sends a SIP INVITE message to the Cisco Unified CME to initiate the call and does not require the user to press the Dial key or wait for the interdigit timeout. To define a dial plan for a SIP phone, perform the following steps.

Before You Begin

- Cisco Unified CME 4.1 or a later version.
- **mode cme** command must be enabled in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dialplan** *dialplan-tag*
4. **type** *phone-type*
5. **pattern** *tag string* [**button** *button-number*] [**timeout** *seconds*] [**user** {**ip** | **phone**}] or **filename** *filename*
6. **exit**
7. **voice register pool** *pool-tag*
8. **dialplan** *dialplan-tag*
9. **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 register dialplan** *dialplan-tag* **Example:** `Router(config)# voice register dialplan 1`	Enters voice register dialplan configuration mode to define a dial plan for SIP phones.
Step 4	**type** *phone-type* **Example:** `Router(config-register-dialplan)# type 7905-7912`	Defines a phone type for the SIP dial plan. • **7905-7912—**Cisco Unified IP Phone 7905, 7905G, 7912, or 7912G. • **7940-7960-others—**Cisco Unified IP Phone 7911, 7940, 7940G, 7941, 7941GE, 7960, 7960G, 7961, 7961GE, 7970, or 7971. • The phone type specified with this command must match the type of phone for which the dial plan is used. If this phone type does not match the type assigned to the phone with the **type** command in voice register pool mode, the dial-plan configuration file is not generated. • You must enter this command before using the **pattern** or **filename** command in the next step.

Step 5	**pattern** *tag string* [**button** *button-number*] [**timeout** *seconds*] [**user** {**ip** | **phone**}] or **filename** *filename*
	
	Example:
	`Router(config-register-dialplan)# pattern 1 52...`
	or
	`Router(config-register-dialplan)# filename dialsip`
		Defines a dial pattern for a SIP dial plan.
		• *tag***—**Number that identifies the dial pattern. Range: 1 to 24.
		• *string***—**Dial pattern, such as the area code, prefix, and first one or two digits of the telephone number, plus wildcard characters or dots (.) for the remainder of the dialed digits.
		• **button** *button-number***—**(Optional) Button to which the dial pattern applies.
		• **timeout** *seconds***—** (Optional) Time, in seconds, that the system waits before dialing the number entered by the user. Range: 0 to 30. To have the number dialed immediately, specify 0. If you do not use this parameter, the phone's default interdigit timeout value is used (10 seconds).
		• **user—**(Optional) Tag that automatically gets added to the dialed number. Do not use this keyword if Cisco Unified CME is the only SIP call agent.
		• **ip—**Uses the IP address of the user.
		• **phone—**Uses the phone number of the user.

	Command or Action	Purpose
		• Repeat this command for each pattern that you want to include in this dial plan. or Specifies a custom XML file that contains the dial patterns to use for the SIP dial plan. • You must load the custom XML file must into flash and the filename cannot include the .xml extension. • The **filename** command is not supported for the Cisco Unified IP Phone 7905 or 7912.
Step 6	**exit** **Example:** `Router(config-register-dialplan)# exit`	Exits dialplan configuration mode.
Step 7	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 4`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone. • *pool-tag*—Unique sequence number of the SIP phone to be configured. Range is version and platform-dependent; type **?** to display range. You can modify the upper limit for this argument by using the the **max-pool** command.
Step 8	**dialplan** *dialplan-tag* **Example:** `Router(config-register-pool)# dialplan 1`	Assigns a dial plan to a SIP phone. • *dialplan-tag*—Number that identifies the dial plan to use for this SIP phone. This is the number that was used with the **voice register dialplan** command in Step 3. Range: 1 to 24.
Step 9	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Examples

The following example shows the configuration for dial plan 1, which is assigned to SIP phone 1:

```
voice register dialplan  1
 type 7940-7960-others
 pattern 1 2... timeout 10 user ip
 pattern 2 1234 user ip button 4
 pattern 3 65...
 pattern 4 1...!
```

```
!
voice register pool  1
 id mac 0016.9DEF.1A70
 type 7961GE
 number 1 dn 1
 number 2 dn 2
 dialplan 1
 dtmf-relay rtp-nte
 codec g711ulaw
```

Troubleshooting Tips for Configuring Dial Plans for SIP

If you create a dial plan by downloading a custom XML dial pattern file to flash and using the **filename** command, and the XML file contains an error, the dial plan might not work properly on a phone. We recommend creating a dial pattern file using the **pattern** command.

To remove a dial plan that was created using a custom XML file with the **filename** command, you must remove the dial plan from the phone, create a new configuration profile, and then use the **reset** command to reboot the phone. You can use the **restart** command after removing a dial plan from a phone only if the dial plan was created using the **pattern** command.

To use KPML if a matching dial plan is not found, when both a dial plan and KPML are enabled on a phone, you must configure a dial pattern with a single wildcard character (.) as the last pattern in the dial plan. For example:

```
voice register dialplan 10
 type 7940-7960-others
 pattern 1 66...
 pattern 2 91.......
```

What to Do Next

If you are done modifying parameters for SIP phones, you must generate a new configuration profile and restart the phones. See Configuration Files for Phones, on page 387.

Verify SIP Dial Plan Configuration

Step 1 **show voice register dialplan** *tag*

This command displays the configuration information for a specific SIP dial plan.

Example:

Router# **show voice register dialplan 1**

```
Dialplan Tag 1
Config:
  Type is 7940-7960-others
  Pattern 1 is 2..., timeout is 10, user option is ip, button is default
  Pattern 2 is 1234, timeout is 0, user option is ip, button is 4
  Pattern 3 is 65..., timeout is 0, user option is phone, button is default
  Pattern 4 is 1..., timeout is 0, user option is phone, button is default
```

Step 2 **show voice register pool** *tag*

This command displays the dial plan assigned to a specific SIP phone.

Example:

Router# **show voice register pool 29**

```
Pool Tag 29
Config:
  Mac address is 0012.7F54.EDC6
  Number list 1 : DN 29
  Proxy Ip address is 0.0.0.0
  DTMF Relay is disabled
  Call Waiting is enabled
  DnD is disabled
  keep-conference is enabled
  dialplan tag is 1
  kpml signal is enabled
  service-control mechanism is not supported
.
.
.
```

Step 3 **show voice register template** *tag*

This command displays the dial plan assigned to a specific template.

Example:

Router# **show voice register template 3**

```
Temp Tag 3
Config:
  Attended Transfer is disabled
  Blind Transfer is enabled
  Semi-attended Transfer is enabled
  Conference is enabled
  Caller-ID block is disabled
  DnD control is enabled
  Anonymous call block is disabled
  Voicemail is 62000, timeout 15
  Dialplan Tag is 1
  Transport type is tcp
```

Enable KPML on a SIP Phone

To enable KPML digit collection on a SIP phone, perform the following steps.

Restriction

- This feature is supported only on Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.
- A dial plan assigned to a phone has priority over KPML.

Before You Begin

Cisco Unified CME 4.1 or a later version.

SUMMARY STEPS

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

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 register pool** *pool-tag* **Example:** `Router(config)# voice register pool 4`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone. • *pool-tag*—Unique sequence number of the SIP phone to be configured. Range is version and platform-dependent; type **?** to display range. You can modify the upper limit for this argument by using the **max-pool** command.
Step 4	**digit collect kpml** **Example:** `Router(config-register-pool)# digit collect kpml`	Enables KPML digit collection for the SIP phone. **Note** This command is enabled by default for supported phones in Cisco Unified CME.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.
Step 6	**show voice register dial-peers** **Example:** `Router# show voice register dial-peers`	Displays details of all dynamically created VoIP dial peers associated with the Cisco Unified CME SIP register, including the defined digit collection method.

What to Do Next

If you are done modifying parameters for SIP phones, you must generate a new configuration profile and restart the phones. See Configuration Files for Phones, on page 387.

Select Session-Transport Protocol for a SIP Phone

To change the session-transport protocol for a SIP phone from the default of UDP to TCP, perform the following steps.

Restriction

- TCP is not supported as a session-transport protocol for the Cisco Unified IP Phone 7905, 7912, 7940, or 7960. If TCP is assigned to an unsupported phone, calls to that phone will not complete successfully. However, the phone can originate calls using UDP, although TCP has been assigned.

Before You Begin

- Cisco Unified CME 4.1 or a later version.
- Directory number must be assigned to SIP phone to which configuration is to be applied. For configuration information, see Assign Directory Numbers to SIP Phones, on page 266.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **session-transport** {**tcp** | **udp**}
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 register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone in Cisco Unified CME.

	Command or Action	Purpose
Step 4	**session-transport** {**tcp** | **udp**} **Example:** `Router(config-register-pool)# session-transport tcp`	(Optional) Specifies the transport layer protocol that a SIP phone uses to connect to Cisco Unified CME. • This command can also be configured in voice register template configuration mode and applied to one or more phones. The voice register pool configuration has priority over the voice register template configuration.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits voice register pool configuration mode and enters privileged EXEC mode.

What to Do Next

Note When TCP is used as session-transport for the SIP phones, and if the TCP Connection aging timer is less than the SIP Register expire timer; then after every TCP connection aging timer expires, the phone will be reset and will re-register to CME. If this is not desired, then modify the TCP Connection aging timer and/or SIP Register expire timer so that SIP Register expire timer is less than TCP Connection aging timer.

- If you want to disable SIP Proxy registration for an individual directory number, see Disable SIP Proxy Registration for a Directory Number, on page 276.
- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Profiles for SIP Phones, on page 391.

Disable SIP Proxy Registration for a Directory Number

To prevent a particular directory number from registering with an external SIP proxy server, perform the following steps.

Restriction Phone numbers that are registered under a voice register dn must belong to a SIP phone that is registered in Cisco Unified CME.

Before You Begin

- Cisco Unified CME 3.4 or a later version.
- Bulk registration is configured at system level. For configuration information, see Configure Bulk Registration, on page 172.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **no-reg**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register dn** *dn-tag* **Example:** `Router(config-register-global)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 4085550152`	Defines a valid number for a directory number to be assigned to a SIP phone in Cisco Unified CME.
Step 5	**no-reg** **Example:** `Router(config-register-dn)# no-reg`	Prevents directory number being configured from registering with an external proxy server.
Step 6	**end** **Example:** `Router(config-register-dn)# end`	Exits voice register dn configuration mode and enters privileged EXEC mode.

What to Do Next

- If you want to configure the G.722-64K codec for all calls through your Cisco Unified CME system, see Modify the Global Codec, on page 278.
- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- If you want to configure individual phones to support some codec other than the system-level codec or some codec other than the phone s native codec, see Codecs for Cisco Unified CME Phones, on page 239.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Profiles for SIP Phones, on page 391.

Modify the Global Codec

To change the global codec from the default (G.711ulaw) to G.722-64K for all calls through Cisco Unified CME, perform the following steps.

Restriction If G.722-64K codec is configured globally and a phone does not support the codec, the fallback codec is G.711ulaw.

Before You Begin

Cisco Unified CME 4.3 or later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **codec** {**g711-ulaw** | **g722-64k**}
5. **service phone g722CodecSupport** {**0** | **1** | **2**}
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.

	Command or Action	Purpose
Step 3	**telephony-service** **Example:** `Router(config)#` **telephony-service**	Enters telephony service configuration mode to set parameters for SCCP and SIP phones in Cisco Unified CME.
Step 4	**codec** {**g711-ulaw** | **g722-64k**} **Example:** `Router(config-telephony)# codec g722-64k`	Specifies the preferred codec for phones in Cisco Unified CME. • Required only if you want to modify codec from the default (G.711ulaw) to G.722-64K.
Step 5	**service phone g722CodecSupport** {**0** | **1** | **2**} **Example:** `Router(config)#` **service phone g722CodecSupport 2**	Causes all phones to advertise the G.722-64K codec to Cisco Unified CME. • Required only if you configured the **codec g722-64k** command in telephony-service configuration mode. • **g722CodecSupport—**Default: 0, phone default set by manufacturer and equal to enabled or disabled. • Cisco phone firmware 8.2.1 or a later version is required to support the G.722-64K codec on G.722-capable SCCP phones. • Cisco phone firmware 8.3.1 or a later version is required to support the G.722-64K codec on G.722-capable SIP phones. • For SCCP only: This command can also be configured in ephone-template configuration mode and applied to one or more SCCP phones.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Exits the telephony service configuration mode and enters privileged EXEC mode.

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- If you want to configure individual phones to support some codec other than the system-level codec or some codec other than the phone s native codec, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- If you are finished configuring SCCP phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Configure Codecs of Individual Phones for Calls Between Local Phones

To designate a codec for individual phones to ensure connectivity between a variety of phones connected to the same Cisco Unified CME router, perform the following steps for each SCCP or SIP phone.

Note If codec values for the dial peers of an internal connection do not match, the call fails. For calls to external phones, that is, phones that are not in the same Cisco Unified CME, such as VoIP calls, the codec is negotiated based on the protocol that is used for the call, such as H.323. Cisco Unified CME plays no part in the negotiation.

Restriction

- Not all phones support all codecs. To verify whether your phone supports a particular codec, see your phone documentation.
- For SIP and SCCP phones in Cisco Unified CME: Modify the configuration for either SIP or SCCP phones to ensure that the codec for all phones match. Do not modify the configuration for both SIP and SCCP phones.
- If G.729 is the desired codec for Cisco ATA-186 and Cisco ATA-188, then only one port of the Cisco ATA device should be configured in Cisco Unified CME. If a call is placed to the second port of the Cisco ATA device, it will be disconnected gracefully. If you want to use both Cisco ATA ports simultaneously, then configure G.711 in Cisco Unified CME.
- If G.722-64K or iLBC codecs are configured in ephone configuration mode and the phone does not support the codec, the fallback is the global codec or G.711ulaw if the global codec is not supported. To configure a global codec, see Modify the Global Codec, on page 278.

Before You Begin

- For SIP phones in Cisco Unified CME: Cisco Unified CME 3.4 or a later version.
- For G.722-64K and iLBC codecs: Cisco Unified CME 4.3 or a later version.
- To support G.722-64K on an individual phone: Cisco phone firmware 8.2.1 or a later version for SCCP phones and 8.3.1 or a later version for SIP phones. For information about upgrading Cisco phone firmware, see Install Cisco Unified CME Software, on page 105 .
- To support iLBC on an individual phone: Cisco phone firmware 8.3.1 or a later version for SCCP and SIP phones. For information about upgrading Cisco phone firmware, see Install Cisco Unified CME Software, on page 105.
- Cisco Unified IP phone to which the codec is to be applied must be already configured. For configuration information for SIP phones, see Assign Directory Numbers to SIP Phones, on page 266. For configuration information for SCCP phones, see Assign Directory Numbers to SCCP Phones, on page 260.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *ephone-tag* or **voice register pool** *pool-tag*
4. **codec** *codec-type*
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** *ephone-tag* or **voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 1**	Enters ephone configuration mode to set phone-specific parameters for a SCCP phone in Cisco Unified CME. or Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone in Cisco Unified CME.

Step 4	**codec** *codec-type*
	
	Example:
	`Router(config-ephone)# codec g729r8`
	`or`
	`Router(config-register-pool)# codec g711alaw`
		Specifies the codec for the dial peer for the IP phone being configured.
		• *codec-type*—Type **?** for a list of codecs.
		• This command overrides any previously configured codec selection set with the **voice-class codec** command.
		• This command overrides any previously configured codec selection set with the **codec** command in telephony-service configuration mode.
		• SCCP only—This command can also be configured in ephone-template configuration mode and applied to one or more phones.

Step 5	**end**
	
	Example:
	`Router(config-ephone)# end`
	or
	`Router(config-register-pool)# end`
		Exits the configuration mode and enters privileged EXEC mode.

What to Do Next

- If you want to select the session-transport protocol for a SIP phone, see Select Session-Transport Protocol for a SIP Phone, on page 275.
- If you are finished configuring SIP phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Profiles for SIP Phones, on page 391.
- If you are finished configuring SCCP phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Configure Phones for a Key System

Creating Directory Numbers for a Simple Key System on SCCP Phone

To create a set of directory numbers with the same number to be associated with multiple line buttons on an IP phone and provide support for call waiting and call transfer on a key system phone, perform the following steps.

Restriction

- Do not configure directory numbers for a key system for dual-line mode because this does not conform to the key system one-call-per-line button usage model for which the phone is designed.
- Provisioning support for the Cisco Unified IP Phone 7931 is available only in Cisco Unified CME 4.0(2) and later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **preference** *preference-order*
6. **no huntstop** or **huntstop**
7. **mwi-type** {**visual** | **audio** | **both**}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 11`	Enters ephone-dn configuration mode to create a directory number.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 101`	Configures a valid phone or extension number for this directory number.
Step 5	**preference** *preference-order* **Example:** `Router(config-ephone-dn)# preference 1`	Sets dial-peer preference order for a directory number associated with a Cisco Unified IP phone. • Default: 0. • Increments the preference order for all subsequent instances within a set of ephone dns with the same number to be associated with a key system phone. That is, the first instance of the directory number is preference **0** by default and you must specify **1** for the second instance of the same number, **2** for the next, and so on. This allows you to create multiple buttons with the same number on an IP phone. • Required to support call waiting and call transfer on a key system phone.

Step 6	**no huntstop** or **huntstop**
	
	Example:
	`Router(config-ephone-dn)# no huntstop`
	or
	`Router(config-ephone-dn)# huntstop`
		Explicitly enables call hunting behavior for a directory number.
		• Configure **no huntstop** for all instances, except the final instance, within a set of ephone dns with the same number to be associated with a key system phone.
		• Required to allow call hunting across multiple line buttons with the same number on an IP phone.
		
		or
		
		Disables call hunting behavior for a directory number.
		• Configure the **huntstop** command for the final instance within a set of ephone dns with the same number to be associated with a key system phone.
		• Required to limit the call hunting to a set of multiple line buttons with the same number on an IP phone.

	Command or Action	Purpose
Step 7	**mwi-type** {**visual** | **audio** | **both**} **Example:** `Router(config-ephone-dn)# mwi-type audible`	Specifies the type of MWI notification to be received. • This command is supported only by Cisco Unified IP Phone 7931s and Cisco Unified IP Phone 7911s. • This command can also be configured in ephone-dn-template configuration mode. The value set in ephone-dn configuration mode has priority over the value set in ephone-dn-template mode.
Step 8	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.

What to Do Next

The following example shows the configuration for six instances of directory number 101, assigned to the first six buttons of an IP phone:

```
ephone-dn 10
 number 101
 no huntstop

ephone-dn 11
 number 101
 preference 1
 no huntstop

ephone-dn 12
 number 101
 preference 2
 no huntstop

ephone-dn 13
 number 101
 preference 3
 no huntstop

ephone-dn 14
 number 101
 preference 4
 no huntstop

ephone-dn 15
 number 101
 preference 5

ephone 1
 mac-address 0001.2345.6789>
 type 7931
 button 1:10 2:11 3:12 4:13 5:14 6:15
```

Configure Trunk Lines for a Key System on SCCP Phone

To set up trunk lines for your key system, perform only one of the following procedures:

- To only enable direct status monitoring of the FXO port on the line button of the IP phone, see Configure a Simple Key System Phone Trunk Line Configuration on SCCP Phone, on page 285.
- To enable direct status monitoring and allow transferred PSTN FXO line calls to be automatically recalled if the transfer target does not answer, see Configure an Advanced Key System Phone Trunk Line Configuration on SCCP Phone, on page 289.

Configure a Simple Key System Phone Trunk Line Configuration on SCCP Phone

Perform the steps in this section to:

- Create directory numbers corresponding to each FXO line that allows phones to have shared or private lines connected directly to the PSTN.
- Enable direct status monitoring of the FXO port on the line button of the IP phone. The line button indicator, either a lamp or an icon depending on the phone, shows the in-use status of the FXO port during the duration of the call.

Restriction

- Directory number with a trunk line cannot be configured for call forward, busy, or no answer.
- Numbers entered after a trunk line is seized will not be displayed. Only the trunk tag is displayed on IP phones.
- Numbers entered after trunk line is seized will not appear in call history or call detail records (CDRs) of a Cisco Unified CME router. Only the trunk tag is logged for calls made from trunk lines.
- FXO trunk lines do not support the CFwdALL, Transfer, Pickup, GPickUp, Park, CallBack, and NewCall softkeys.
- FXO trunk lines do not support conference initiator dropoff.
- FXO trunk lines do not support on-hook redial. The phone user must explicitly select the FXO trunk line before pressing the Redial button.
- FXO trunk lines do not support call transfer to IP phones. However, the call initiator can conference an FXO line with an IP phone by pressing the Hold button, which leaves the FXO trunk line and IP phone connected. The conference initiator is unable to participate in the conference, but can place calls on other lines.
- FXO trunk lines do not support bulk speed dial.
- FXO port monitoring has the following restrictions:
    - Not supported before Cisco Unified CME 4.0.
    - Supported only for analog FXO loop-start and ground-start ports and T1/E1 FXO CAS ports. FXS loop-start and ground-start ports and PRI/BRI PSTN trunks are not supported.
    - Not supported for analog ports on the Cisco VG224 or Cisco ATA 180 Series.
    - T1 CAS DS0 group must be configured per time slot (cannot bundle more than one time slot into a ds0-group).
- Transfer recall and transfer-to button optimization are supported on dual-line directory numbers only in Cisco Unified CME 4.0 and later versions.
- Transfer-to button optimization is not supported for call forwarding, call-park recall, call pickup on hold, or call pickup at alert.

Before You Begin

- FXO port for a private line automatic ringdown (PLAR) off-premises extension (OPX) connection must be configured; for example:

```
voice-port 1/0/0
 connection p lar-opx 801 <<----Private number
```

- Dial peers for FXO port must be configured; for example:

```
dial-peer voice 111 pots
 destination-pattern 811 <<----Trunk-tag
 port 1/0/0
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **trunk** *trunk-tag* [**timeout** *seconds*] **monitor-port** *port*
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	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 51`	Enters ephone-dn configuration mode to create a directory number. • Configure this command in the default single line mode, without the **dual-line** keyword, when configuring a simple key system trunk line.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 801`	Configures a valid phone or extension number for this directory number.
Step 5	**trunk** *trunk-tag* [**timeout** *seconds*] **monitor-port** *port* **Example:** `Router(config-ephone-dn)# trunk 811 monitor-port 1/0/0`	Associates a directory number with an FXO port. • The **monitor-port** keyword is not supported before Cisco Unified CME 4.0. • The **monitor-port** keyword is not supported on directory numbers for analog ports on the Cisco VG224 or Cisco ATA 180 Series.
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Examples

The following example shows the configuration for six instances of directory number 101, assigned to the first six buttons of an IP phone, plus four PSTN line appearances that are assigned to buttons 7 to 10:

```
ephone-dn 10
 number 101
 no huntstop

ephone-dn 11
 number 101
 preference 1
 no huntstop

ephone-dn 12
 number 101
 preference 2
 no huntstop

ephone-dn 13
 number 101
 preference 3
 no huntstop

ephone-dn 14
 number 101
 preference 4
 no huntstop

ephone-dn 15
 number 101
 preference 5

ephone-dn 51
 number 801
 trunk 811 monitor-port 1/0/0>

ephone-dn 52
 number 802
 trunk 812 monitor-port 1/0/1

ephone-dn 53
 number 803
 trunk 813 monitor-port 1/0/2

ephone-dn 54
 number 804
 trunk 814 monitor-port 1/0/3

ephone 1
 mac-address 0001.2345.6789
 type 7931
 button 1:11 2:12 3:13 4:14 5:15 6:16 7:51 8:52 9:53 10:54

voice-port 1/0/0
 connection plar opx 801

voice-port 1/0/1
 connection plar opx 802

voice-port 1/0/2
 connection plar opx 803

voice-port 1/0/3
 connection plar opx 804

dial-peer voice 811 pots
 destination-pattern 811
 port 1/0/0

dial-peer voice 812 pots
```

```
 destination-pattern 812
 port 1/0/1

dial-peer voice 813 pots
 destination-pattern 813
 port 1/0/2

dial-peer voice 814 pots
 destination-pattern 814
 port 1/0/3
```

What to Do Next

You are ready to configure each individual phone and assign button numbers, line characteristics, and directory numbers to buttons on the phone. See Configure Individual IP Phones for Key System on SCCP Phone, on page 293.

Configure an Advanced Key System Phone Trunk Line Configuration on SCCP Phone

Perform the steps in this section to:

- Create directory numbers corresponding to each FXO line that allows phones to have shared or private lines connected directly to the PSTN.
- Enable direct status monitoring of the FXO port on the line button of the IP phone. The line button indicator, either a lamp or an icon depending on the phone, shows the in-use status of the FXO port during the duration of the call.
- Allow transferred PSTN FXO line calls to be automatically recalled if the transfer target does not answer after the specified number of seconds. The call is withdrawn from the transfer-to phone and the call resumes ringing on the phone that initiated the transfer.

Restriction

- Ephone-dn with a trunk line cannot be configured for call forward, busy, or no answer.
- Numbers entered after a trunk line is seized will not be displayed. Only the trunk tag is displayed on IP phones.
- Numbers entered after a trunk line is seized will not appear in call history or call detail records (CDRs) of a Cisco Unified CME router. Only the trunk tag is logged for calls made from trunk lines.
- FXO trunk lines do not support the CFwdALL, Transfer, Pickup, GPickUp, Park, CallBack, and NewCall softkeys.
- FXO trunk lines do not support conference initiator dropoff.
- FXO trunk lines do not support on-hook redial. The phone user must explicitly select the FXO trunk line before pressing the Redial button.
- FXO trunk lines do not support call transfer to IP phones. However, the call initiator can conference an FXO line with an IP phone by pressing the Hold button, which leaves the FXO trunk line and IP phone connected. The conference initiator is unable to participate in the conference, but can place calls on other lines.
- FXO trunk lines do not support bulk speed dial.
- FXO port monitoring has the following restrictions:
    - Not supported before Cisco Unified CME 4.0.
    - Supported only for analog FXO loop-start and ground-start ports and T1/E1 FXO CAS ports. FXS loop-start and ground-start ports and PRI/BRI PSTN trunks are not supported.
    - Not supported for analog ports on the Cisco VG224 or Cisco ATA 180 Series.
    - T1 CAS DS0 group must be configured per time slot (cannot bundle more than one time slot into a ds0-group).
- Transfer recall and transfer-to button optimization is supported on dual-line directory numbers only in Cisco Unified CME 4.0 and later.
- Transfer-to button optimization is not supported for call forwarding, call-park recall, call pickup on hold, or call pickup at alert.
- Transfer recall is not supported for analog ports on the Cisco VG224 or Cisco ATA 180 Series.

Before You Begin

- FXO port for a private line automatic ringdown (PLAR) off-premises extension (OPX) connection must be configured; for example:

```
voice-port 1/0/0
 connection plar-opx 801 <<----Private number
```

- Dial peers for FXO port must be configured; for example:

```
dial-peer voice 111 pots
 destination-pattern 811 <<----Trunk-tag
 port 1/0/0
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* **dual-line**
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **trunk** *digit-string* [**timeout** *seconds*] [**transfer-timeout** *seconds*] [**monitor-port** *port*]
6. **huntstop** [**channel**]
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	**ephone-dn** *dn-tag* **dual-line** **Example:** `Router(config)# ephone-dn 51 dual-line`	Enters ephone-dn configuration mode for the purpose of creating and configuring a telephone or extension number. • **dual-line**—Required when configuring an advanced key system phone trunk line. Dual-line mode provides a second call channel for the directory number on which to place an outbound consultation call during the call transfer attempt. This also allows the phone to remain part of the call to monitor the progress of the transfer attempt and if the transfer is not answered, to pull the call back to the phone on the original PSTN line button.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 801`	Configures a valid telephone number or extension number for this directory number.
Step 5	**trunk** *digit-string* [**timeout** *seconds*] [**transfer-timeout** *seconds*] [**monitor-port** *port*] **Example:** `Router(config-ephone-dn)# trunk 811 transfer-timeout 30 monitor-port 1/0/0`	Associates this directory number with an FXO port. • **transfer-timeout** *seconds*—For dual-line ephone-dns only. Range: 5 to 60000. Default: Disabled. • The **monitor-port** keyword is not supported before Cisco Unified CME 4.0.

	Command or Action	Purpose
		• The **monitor-port** and **transfer-timeout** keywords are not supported on directory numbers for analog ports on the Cisco VG224 or Cisco ATA 180 Series.
Step 6	**huntstop** [**channel**] **Example:** `Router(config-ephone-dn)# huntstop channel`	Disables call hunting to the second channel of this directory number if the first channel is busy or does not answer. • **channel—**Required when configuring an advanced key system phone trunk line. Reserves the second channel created by configuring dual-line mode for the **ephone-dn** command so that an outbound consultation call can be placed during a call transfer attempt.
Step 7	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.

Examples

The following example shows the configuration for six instances of directory number 101, assigned to the first six buttons of an IP phone, plus four PSTN line appearances that are assigned to buttons 7 to 10. These four PSTN line appearances are configured as dual lines to provide a second call channel on which to place an outbound consultation call during a call transfer attempt. This configuration allows the phone to remain part of the call to monitor the progress of the transfer attempt, and if the transfer is not answered, to pull the call back to the phone on the original PSTN line button.

```
ephone-dn 10
 number 101
 no huntstop

ephone-dn 11
 number 101
 preference 1
 no huntstop

ephone-dn 12
 number 101
 preference 2
 no huntstop

ephone-dn 13
 number 101
 preference 3
 no huntstop

ephone-dn 14
 number 101
 preference 4
 no huntstop

ephone-dn 15
 number 101
 preference 5

ephone-dn 51 dual-line
```

```
 number 801
 trunk 811 transfer-timeout 30 monitor-port 1/0/0
 huntstop channel

ephone-dn 52 dual-line
 number 802
 trunk 812 transfer-timeout 30 monitor-port 1/0/1
 huntstop channel

ephone-dn 53 dual-line
 number 803
 trunk 813 transfer-timeout 30 monitor-port 1/0/2
 huntstop channel

ephone-dn 54 dual-line
 number 804>
 trunk 814 transfer-timeout 30 monitor-port 1/0/3
 huntstop channel

ephone 1
 mac-address 0001.2345.6789
 type 7931
 button 1:11 2:12 3:13 4:14 5:15 6:16 7:51 8:52 9:53 10:54

voice-port 1/0/0
 connection plar opx 801

voice-port 1/0/1
 connection plar opx 802

voice-port 1/0/2
 connection plar opx 803

voice-port 1/0/3
 connection plar opx 804

dial-peer voice 811 pots
 destination-pattern 811
 port 1/0/0

dial-peer voice 812 pots
 destination-pattern 812
 port 1/0/1

dial-peer voice 813 pots
 destination-pattern 813
 port 1/0/2

dial-peer voice 814 pots
 destination-pattern 814
 port 1/0/3
```

Configure Individual IP Phones for Key System on SCCP Phone

To assign button numbers, line characteristics, and directory numbers to buttons on an individual phone that will operate as a key system phone, perform the following steps.

Restriction

- Provisioning for Cisco Unified IP Phone 7931G is available only in Cisco Unified CME 4.0(2) and later versions.
- Cisco Unified IP Phone 7931G can support only one call waiting overlaid per directory number.
- Cisco Unified IP Phone 7931G cannot support overlays that contain directory numbers configured for dual-line mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mac-address** [*mac-address*]
5. **type** *phone-type*
6. **button** *button-number* {*separator*} *dn-tag* [,*dn-tag*...] [*button-number*{**x**}*overlay-button-number*] [*button-number*...]
7. **mwi-line** *line-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	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode.
Step 4	**mac-address** [*mac-address*] **Example:** `Router(config-ephone)# mac-address 0001.2345.6789`	Specifies the MAC address of the IP phone that is being configured.

	Command or Action	Purpose
Step 5	**type** *phone-type* **Example:** `Router(config-ephone)# type 7931`	Specifies the type of phone that is being configured.
Step 6	**button** *button-number* {*separator*} *dn-tag* [,*dn-tag*...] [*button-number*{**x**}*overlay-button-number*] [*button-number*...] **Example:** `Router(config-ephone)# button 1:11 2:12 3:13 4:14 5:15 6:16 7:51 8:52 9:53 10:54`	Associates a button number and line characteristics with an ephone-dn. Maximum number of buttons is determined by phone type. **Tip** The line button layout for the Cisco Unified IP Phone 7931G is a bottom-up array. Button 1 is at the bottom right of the array and button 24 is at the top left of the array.
Step 7	**mwi-line** *line-number* **Example:** `Router(config-ephone)# mwi-line 3`	Selects a phone line to receive MWI treatment; when a message is waiting for the selected line, the message waiting indicator is activated. • *line-number*—Range: 1 to 34. Default: 1.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Exits ephone configuration mode and enters privileged EXEC mode.

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see Select Button Layout for a Cisco Unified SCCP IP Phone 7931G, on page 1453.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Configure Cisco ATA, Analog Phone Support, Remote Phones, Cisco IP Communicator, and Secure IP Phone (IP-STE)

Configure Cisco ATA Support

To enable an analog phone that uses a Cisco ATA to register with Cisco Unified CME, perform the following steps.

Restriction For a Cisco ATA that is registered to a Cisco Unified CME system to participate in fax calls, it must have its ConnectMode parameter set to use the same RTP payload type as the Cisco voice gateway that is performing the fax pass-through. Cisco voice gateways use standard payload type 0/8, which is selected on Cisco ATAs by setting bit 2 of the ConnectMode parameter to 1. For more information, see the *Parameters and Defaults* chapter in Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0).

Step 1 Install the Cisco ATA.
See the *Installing the Cisco ATA* chapter in Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0).

Step 2 Configure the Cisco ATA.
See the *Configuring the Cisco ATA for SCCP* chapter in Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0).

Step 3 Upgrade the firmware to the latest Cisco ATA image.
If you are using either the v2.14 or v2.14ms Cisco ATA 186 image based on the 2.14 020315a build for H.323/SIP or the 2.14 020415a build for MGCP or SCCP, you must upgrade to the latest version to install a security patch. This patch fixes a security hole in the Cisco ATA Web server that allows users to bypass the user interface password.

For information about upgrading firmware, see Install Cisco Unified CME Software, on page 105. Alternatively, you can use a manual method, as described in the *Upgrading the Cisco ATA Signaling Image* chapter of Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0).

Step 4 Set the following network parameters on the Cisco ATA:

- DHCP parameter to **1** (enabled).
- TFTP parameter to **1** (enabled).
- TFTPURL parameter to the IP address of the router running Cisco Unified CME.
- SID0 parameter to a period (**.**) or the MAC address of the Cisco ATA (to enable the first port).
- SID1 parameter to a period (**.**) or a modified version the Cisco ATA's MAC address, with the first two hexadecimal numbers removed and 01 appended to the end, if you want to use the second port. For example, if the MAC address of the Cisco ATA is 00012D01073D, set SID1 to 012D01073D01.
- Nprintf parameter to the IP address and port number of the host to which all Cisco ATA debug messages are sent. The port number is usually set to 9001.
- To prevent tampering and unauthorized access to the Cisco ATA 186, you can disable the web-based configuration. However, if you disable the web configuration page, you must use either a TFTP server or the voice configuration menu to configure the Cisco ATA 186.

Step 5 In Cisco Unified CME, configure analog phones that use a Cisco ATA in the same way as a Cisco Unified IP phone. In the **type** command, use the **ata** keyword. For information on how to provision phones, see Create Directory Numbers for SCCP Phones, on page 253.

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see Select Button Layout for a Cisco Unified SCCP IP Phone 7931G, on page 1453.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388 and Generate Configuration Profiles for SIP Phones, on page 391.

Verify Cisco ATA Support

Use the **show ephone ata** command to display SCCP phone configurations with the **type ata** command.

The following is sample output for a Cisco Unified CME configured for two analog phones using a Cisco ATA with MAC address 000F.F758.E70E:

```
  ephone-30 Mac:000F.F758.E70E TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 1 and
Server in ver 1
  mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
  IP:1.4.188.72 15325 ATA Phone  keepalive 7 max_line 2 dual-line
  button 1: dn 80 number 8080 CH1   IDLE         CH2 IDLE

  ephone-31 Mac:0FF7.58E7.0E01 TCP socket:[3] activeLine:0 REGISTERED in SCCP ver 1 and
Server in ver 1
  mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:3
  IP:1.4.188.72 15400 ATA Phone  keepalive 7 max_line 2 dual-line
  button 1: dn 81 number 8081 CH1   IDLE         CH2 IDLE
```

Troubleshooting Cisco ATA Support

Use the **debug ephone detail** command to diagnose problems with analog phones that use Cisco ATAs.

Call Pickup and Group Call Pickup with Cisco ATA

Most of the procedures for using Cisco ATAs with Cisco Unified CME are the same as those for using Cisco ATAs with Cisco Unified Communications Manager, as described in the *How to Use Pre-Call and Mid-Call Services* chapter of Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0). However, the call pickup and group call pickup procedures are different when using Cisco ATAs with Cisco Unified CME, as described below:

Call Pickup

When using Cisco ATAs with Cisco Unified CME:

- To pickup the last parked call, press ****3***.
- To pickup a call on a specific extension, press ****3** and enter the extension number.
- To pickup a call from a park slot, press ****3** and enter the park slot number.

Group Call Pickup

When using Cisco ATAs with Cisco Unified CME:

- To answer a phone within your call pickup group, press ****4***.
- To answer a phone outside of your call pickup group, press ****4** and the group ID number.

Note If there is only one pickup group, you do not need to enter the group ID after the ****4** to pickup a call.

Configure Voice and T.38 Fax Relay on Cisco ATA-187

Restriction

- H.323 trunk calls are not supported.
- Hardware conferencing with DSPFarm resource is not supported on Cisco ATA-187 in Cisco Unified CME 9.0. With the correct firmware (9.2(3) or a later version), local three-way conferencing is supported.

Before You Begin

Cisco Unified CME 9.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **authenticate realm** *string*
5. **exit**
6. **voice service** {**voip** | **voatm**}
7. **allow-connections** *from-type* **to** *to-type*
8. **fax protocol t38** [**ls_redundancy** *value* [**hs_redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
9. **exit**
10. **voice register pool** *pool-tag*
11. **id mac** *address*
12. **type** *phone-type*
13. **ata-ivr-pwd** *password*
14. **session-transport** {**tcp** | **udp**}
15. **number** *tag* **dn** *dn-tag*
16. **username** *username* [**password** *password*]
17. **codec** *codec-type* [*bytes*]
18. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 4	**authenticate realm** *string* **Example:** `Router(config-register-global)# authenticate realm xxxxx`	• **realm** *string*—Realm parameter for challenge and response as specified in RFC 2617 is authenticated.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global configuration mode.
Step 6	**voice service** {**voip** | **voatm**} **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode to specify a voice encapsulation type. • **voip**—Specifies Voice over IP (VoIP) parameters. • **voatm**—Specifies Voice over ATM (VoATM) parameters.

Step 7	**allow-connections** *from-type* **to** *to-type*
	
	Example:
	`Router(config-voi-serv)# allow-connections sip to sip`
		Allows connections between specific types of endpoints in a VoIP network.
		• *from-type*—Originating endpoint type. The following choices are valid:
		  ◦ **sip**—Session Interface Protocol.
		• **to**—Indicates that the argument that follows is the connection target.
		• *to-type*—Terminating endpoint type. The following choices are valid:
		  ◦ **sip**—Session Interface Protocol.

Step 8	**fax protocol t38** [**ls_redundancy** *value* [**hs_redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
	
	Example:
	`Router(config-voi-serv)# fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback pass-through g711ulaw`
		Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
		• **ls_redundancy** *value*—(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. Default is 0.
		• **hs_redundancy** *value*—(Optional) (T.38 fax relay only) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. Default is 0.
		• **fallback**—(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.
		• **pass-through**—(Optional) The fax stream uses one of the following high-bandwidth codecs:
		  ◦ **g711ulaw**—Uses the G.711 u-law codec.
		  ◦ **g711alaw**—Uses the G.711 a-law codec.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits voice-service configuration mode.
Step 10	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 11`	Enters voice register pool configuration mode to set phone-specific parameters for a Cisco Unified SIP phone in Cisco Unified CME. • *pool-tag*—Unique number assigned to the pool. Range: 1 to 100.
Step 11	**id mac** *address* **Example:** `Router(config-register-pool)# id mac 93FE.12D8.2301`	identifies a locally available Cisco Unified SIP IP phone. • **mac** *address*—Identifies the MAC address of a particular Cisco Unified SIP IP phone.
Step 12	**type** *phone-type* **Example:** `Router(config-register-pool)# type ATA-187`	Defines a phone type for the SIP phone being configured.
Step 13	**ata-ivr-pwd** *password* **Example:** `Router(config-register-pool)# ata-ivr-pwd 1234`	(Optional) Defines a password to access interactive voice response (IVR) and change the default phone settings on Cisco Analog Telephone Adaptors. • *password*—Four-digit or five-digit string to be used as password to access IVR. Password string must contain numbers 0 to 9.
Step 14	**session-transport** {**tcp** | **udp**} **Example:** `Router(config-register-pool)# session-transport tcp`	(Optional) Specifies the transport layer protocol that a Cisco Unified SIP IP phone uses to connect to Cisco Unified CME. • **tcp**—Transmission Control Protocol (TCP) is used. • **udp**—User Datagram Protocol (UDP) is used. This is the default.
Step 15	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 33`	Indicates the E.164 phone numbers that the registrar permits to handle the Register message from the Cisco Unified SIP IP phone. • *tag*—Identifies the telephone number when there are multiple number commands. Range: 1 to 10. • **dn** *dn-tag*—Identifies the directory number tag for this phone number as defined by the voice register dn command. Range: 1 to 150.
Step 16	**username** *username* [**password** *password*] **Example:** `Router(config-register-pool)# username ata112 password cisco`	Assigns an authentication credential to a phone user so that the SIP phone can register in Cisco Unified CME. • *username*—Username of the local Cisco IP phone user. Default: Admin. • **password**—Enables password for the Cisco IP phone user.

	Command or Action	Purpose
		• *password*—Password string.
Step 17	**codec** *codec-type* [*bytes*] **Example:** `Router(config-register-pool)# codec g711ulaw`	Specifies the codec to be used when setting up a call for a SIP phone or group of SIP phones in Cisco Unified CME. • *codec-type*—Preferred codec; values are as follows: ◦ **g711alaw**—G.711 A law 64K bps. ◦ **g711ulaw**—G.711 micro law 64K bps. ◦ **g722r64**—G.722-64K at 64K bps. ◦ **g729r8**—G.729 8K bps (default). ◦ **ilbc**— internet Low Bitrate Codec (iLBC) at 13,330 bps or 15,200 bps.
Step 18	**end** **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.

Auto-Configuration for Cisco VG202, VG204, and VG224

Restriction Supported only for the Cisco VG202, VG204, and VG224 voice gateways.

Before You Begin

- Cisco Unified CME 7.1 or a later version. The Cisco Unified CME router must be configured and running before you boot the analog voice gateway. See Set Up Cisco Unified CME for SCCP Phones , on page 175.
- Default location of configuration files is system:/its/. To define an alternate location at which to save the gateway configuration files, see Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- To automatically assign the next available directory number to the voice port as it registers to Cisco Unified CME, and create an ephone entry associated with each voice port, enable the **auto assign** command in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-gateway system** *tag*
4. **mac-address** *mac-address*
5. **type** {**vg202** | **vg204** | **vg224**}
6. **voice-port** *port-range*
7. **network-locale** *locale-code*
8. **create cnf-files**
9. **reset** or **restart**
10. **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-gateway system** *tag* **Example:** `Router(config)# voice-gateway system 1`	Enters voice gateway configuration mode and creates a voice gateway configuration.
Step 4	**mac-address** *mac-address* **Example:** `Router(config-voice-gateway)# mac-address`	Defines the MAC address of the voice gateway to autoconfigure.
Step 5	**type** {**vg202** | **vg204** | **vg224**} **Example:** `Router(config-voice-gateway)# type vg224`	Defines the type of voice gateway to autoconfigure.
Step 6	**voice-port** *port-range* **Example:** `Router(config-voice-gateway)# voice-port 0-23`	Identifies the ports on the voice gateway that register to Cisco Unified CME.

	Command or Action	Purpose
Step 7	**network-locale** *locale-code* **Example:** `Router(config-voice-gateway)# network-locale FR`	Selects a geographically specific set of tones and cadences for the voice gateway s analog endpoints that register to Cisco Unified CME.
Step 8	**create cnf-files** **Example:** `Router(config-voice-gateway)# create cnf-files`	Generates the XML configuration files that are required for the voice gateway to autoconfigure its analog ports that register to Cisco Unified CME.

Step 9	**reset** or **restart**
	
	Example:
	`Router(config-voice-gateway)# reset`
	or
	`Router(config-voice-gateway)# restart`
		(Optional) Performs a complete reboot of all analog phones associated with the voice gateway and registered to Cisco Unified CME.
		
		or
		
		(Optional) Performs a fast restart of all analog phones associated with the voice gateway after simple changes to buttons, lines, or speed-dial numbers.
		
		• Use these commands to download new configuration files to the analog phones after making configuration changes to the phones in Cisco Unified CME.

Step 10	**end** **Example:** `Router(config-voice-gateway)# end`	Exits to privileged EXEC mode.

The following example shows the voice gateway configuration in Cisco Unified CME:

```
voice-gateway system  1
 network-locale FR
 type VG224
 mac-address 001F.A30F.8331
 voice-port 0-23
 create cnf-files
```

What to Do Next

- Cisco VG202 or VG204 voice gateway Enable the gateway for autoconfiguration. See the *Auto-Configuration on the Cisco VG202 and Cisco VG204 Voice Gateways* section in Cisco VG202 and Cisco VG204 Voice Gateways Software Configuration Guide.
- Cisco VG224 analog phone gateway Enable SCCP and the STC application on the gateway. See the *Configuring FXS Ports for Basic Calls* chapter in Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

Configure Phones on SCCP Controlled Analog (FXS) Ports

Configuring Cisco Unified CME to support calls and features on analog endpoints connected to SCCP controlled analog (FXS) ports is basically the same as configuring any SCCP phone in Cisco Unified CME. This section describes only the steps that have special meaning for phones connected to a Cisco VG224 Analog Phone Gateway.

Restriction FXS ports on Cisco VG248 analog phone gateways are not supported by Cisco Unified CME.

Before You Begin

- For phones connected to analog FXS ports on the Cisco VG224 Analog Phone Gateway: Cisco CME 3.2.2 or a later version.
- For phones connected to analog FXS ports on the Cisco Integrated Services Routers (ISR) voice gateway: Cisco Unified CME 4.0 or a later version.
- Cisco ISR voice gateway or Cisco VG224 analog phone gateway is installed and configured for operation. For information, see the appropriate Cisco configuration documentation.
- Prior to Cisco IOS Release 12.4(11)T, set the **timeouts ringing** command to **infinity** for all SCCP-controlled analog ports. In Cisco IOS Release 12.4(11)T and later, the default for this command is infinity.
- SCCP is enabled on the Cisco IOS voice gateway. For configuration information, see Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

Step 1 Set up ephone-dns for up to 24 endpoints on the Cisco IOS gateway.
Use the **ephone-dn** command:

Example:

```
ephone-dn 1 dual-line
 number 1000
.
.
.
ephone-dn 24 dual-line
 number 1024
```

Step 2 Set the maximum number of ephones.
Use the **max ephones** command to set a number equal to or greater than the total number of endpoints that you intend to register on the Cisco Unified CME router, including both IP and analog endpoints. For example, if you have 6 IP phones and 12 analog phones, set the **max ephones** command to 18 or greater.

Step 3 Assign ephone-dns to ephones.
Use the **auto assign** command to enable the automatic assignment of an available ephone-dn to each phone as the phone contacts the Cisco Unified CME router to register.

Note The order of ephone-dn assignment is not guaranteed. For example, if you have analog endpoints on ports 2/0 through 2/23 on the Cisco IOS gateway, port 2/0 does not necessarily become ephone 1. Use one of the following commands to enable automatic ephone-dn assignment.

- **auto assign 1 to 24**—You do not need to use the **type** keyword if you have only analog endpoints to be assigned or if you want all endpoints to be automatically assigned.
- **auto assign 1 to 24 type anl**—Use the **type** keyword if you have other phone types in the system and you want only the analog endpoints to be assigned to ephone-dns automatically.

An alternative to using the **auto assign** command is to manually assign ephone-dns to ephones (analog phones on FXS ports). This method is more complicated, but you might need to use it if you want to assign a specific extension number (ephone-dn) to a particular ephone. The reason that manual assignment is more complicated is because a unique device ID is required for each registering ephone and analog phones do not have unique MAC addresses like IP phones do. To create unique device IDs for analog phones, the auto assign process uses a particular algorithm. When you make manual ephone assignments, you have to use the same algorithm for each phone that receives a manual assignment.

The algorithm uses the single 12-digit SCCP local interface MAC address on the Cisco IOS gateway as the base to create unique 12-digit device IDs for all the FXS ports on the Cisco IOS gateway. The rightmost 9 digits of the SCCP local interface MAC address are shifted left three places and are used as the leftmost 9 digits for all 24 individual device IDs. The remaining 3 digits are the hexadecimal translation of the binary representation of the port's slot number (3 digits), subunit number (2 digits), and port number (7 digits). The following example shows the use of the algorithm to create a unique device ID for one port:

1. The MAC address for the Cisco VG224 SCCP local interface is 000C.8638.5EA6.
2. The FXS port has a slot number of 2 (010), a subunit number of 0 (00), and a port number of 1 (0000001). The binary digits are strung together to become 0100 0000 0001, which is then translated to 401 in hexadecimal to create the final device ID for the port and ephone.
3. The resulting unique device ID for this port is C863.85EA.6401.

When manually setting up an ephone configuration for an analog port, assign it just one button because the port represents a single-line device. The **button** command can use the ":" (colon, for normal), "o" (overlay) and "c" (call-waiting overlay) modes.

Note Once you have assigned ephone-dns to all the ephones that you want to assign manually, you can use the **auto assign** command to automatically assign the remaining ports.

Step 4 Set up feature parameters as desired.
The following list includes commonly configured features. For information about supported features, see Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

- Call transfer—To use call transfer from analog endpoints, the **transfer-system** command must be configured for the **full-blind** or**full-consult** keyword in telephony-service configuration mode on the Cisco Unified CME router. This is the recommended setting for Cisco CME 3.0 and later versions, but it is not the default.
- Call forwarding—Call forwarding destinations are specified for all, busy, and no-answer conditions for each ephone-dn using the **call-forward all**, **call-forward busy**, and **call-forward noan** commands in ephone-dn configuration mode.
- Call park—Call-park slots are created using the **park-slot** command in ephone-dn configuration mode. Phone users must be instructed how to transfer calls to the call-park slots and use directed pickup to retrieve the calls.
- Call pickup groups—Extensions are added to pickup groups using the **pickup-group** command in ephone-dn configuration mode. Phone users must be told which phones are in which groups.

- Caller ID—Caller names are defined using the **name** command in ephone-dn configuration mode. Caller numbers are defined using the **number** command in ephone-dn configuration mode.
- Speed dial—Numbers to be speed-dialed are stored with their associated speed-dial codes using the **speed-dial** command in ephone configuration mode.
- Speed dial to voice mail—The voice-mail number is defined using the **voicemail** command in telephony-service configuration mode.

Step 5 Set up feature restrictions as desired.
Features such as transfer, conference, park, pickup, group pickup (gpickup), and call forward all (cfwdall) can be restricted from individual ephones using the appropriate Cisco Unified CME softkey template command, even though analog phones do not have softkeys. Simply create a template that leaves out the softkey that represents the feature you want to restrict and apply the template to the ephone for which you want the feature restricted. For more information about softkey template customization, see Customize Softkeys, on page 925.

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see Select Button Layout for a Cisco Unified SCCP IP Phone 7931G, on page 1453.
- After configuring phones in Cisco Unified CME to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Verify Analog Phone Support

Use the following **show** commands to display information about analog endpoints.

- **show ephone anl**—Displays MAC address, registration status, ephone-dn, and speed-dial numbers for analog ephones.
- **show telephony-service ephone-dn**—Displays call forward, call waiting, pickup group, and more information about ephone-dns.
- **show running-config**—Displays running configuration nondefault values.

Enable Remote Phone

To enable IP phones or instances of Cisco IP Communicator to connect to a Cisco Unified CME system over a WAN, perform the following steps.

Restriction

- Because Cisco Unified CME is not designed for centralized call processing, remote phones are supported only for fixed teleworker applications, such as working from a home office.
- Cisco Unified CME does not support CAC for remote SCCP phones, so voice quality can degrade if a WAN link is oversubscribed. High-bandwidth data applications used over a WAN can cause degradation of voice quality for remote IP phones.
- Cisco Unified CME does not support Emergency 911 (E911) calls from remote IP phones. Teleworkers using remote phones connected to Cisco Unified CME over a WAN should be advised not to use these phones for E911 emergency services because the local public safety answering point (PSAP) will not be able to obtain valid calling-party information from them.

  We recommend that you make all remote phone users aware of this issue. One way is to place a label on all remote teleworker phones that reminds users not to place 911 emergency calls on remote IP phones. Remote workers should place any emergency calls through locally configured hotel, office, or home phones (normal land-line phones) whenever possible. Inform remote workers that if they must use remote IP phones for emergency calls, they should be prepared to provide specific location information to the answering PSAP personnel, including street address, city, state, and country.

Before You Begin

- The WAN link supporting remote teleworker phones should be configured with a Call Admission Control (CAC) or Resource Reservation Protocol (RSVP) solution to prevent the oversubscription of bandwidth, which can degrade the quality of all voice calls.
- If DSP farms will be used for transcoding, you must configure them separately. See Configure Transcoding Resources, on page 479.
- A SCCP phone to be enabled as a remote phone is configured in Cisco Unified CME. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mtp**
5. **codec** {**g711ulaw** | **g722r64** | **g729r8** [**dspfarm-assist**]}
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 4	**mtp** **Example:** `Router(config-ephone)# mtp`	Sends media packets to the Cisco Unified CME router.
Step 5	**codec** {**g711ulaw** | **g722r64** | **g729r8** [**dspfarm-assist**]} **Example:** `Router(config-ephone)# codec g729r8 dspfarm-assist`	(Optional) Selects a preferred codec for setting up calls. • Default: G.711 mu-law codec. • The **g722r64** keyword requires Cisco Unified CME 4.3 and later versions. • **dspfarm-assist**—Attempts to use DSP-farm resources for transcoding the segment between the phone and the Cisco Unified CME router if G.711 is negotiated for the call. **Note** The **dspfarm-assist** keyword is ignored if the SCCP endpoint type is ATA, VG224, or VG248.
Step 6	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

What to Do Next

- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see Configure Codecs of Individual Phones for Calls Between Local Phones, on page 280.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see Select Button Layout for a Cisco Unified SCCP IP Phone 7931G, on page 1453.
- After configuring phones in Cisco Unified CME to make basic calls, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Verify Remote Phones

Use the **show running-config** command or the **show telephony-service ephone** command to verify parameter settings for remote ephones.

Configure Cisco IP Communicator Support on SCCP Phone

To enable support for Cisco IP Communicator, perform the following steps.

Before You Begin

- Cisco Unified CME 4.0 or a later version.
- IP address of the Cisco Unified CME TFTP server.
- PC for Cisco IP Communicator is installed. For hardware and platform requirements, see the appropriate Cisco IP Communicator User Guide.
- Audio devices, such as headsets and handsets for users, are installed. You can install audio devices any time, but the ideal time to do this is before you install and launch Cisco IP Communicator.
- Directory numbers and ephone configuration for Cisco IP Communicator are configured in Cisco Unified CME. For information, see Configure Phones for a PBX System, on page 253.

Step 1 Download Cisco IP Communicator 2.0 or a later version software from the software download site at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Step 2 Install the software on your PC, then launch the Cisco IP Communicator application.
For information, see the *Installing and Launching Cisco IP Communicator* section in the appropriate Cisco IP Communicator User Guide.

Step 3 Complete the configuration and registration tasks on the Cisco IP Communicator as required, including the following:

a) Configure the IP address of the Cisco Unified CME TFTP server.
   - Right-click on the Cisco IP Communicator interface, then choose **Preferences** > **Network** > **Use these TFTP servers**.
   - Enter the IP address of the Cisco Unified CME TFTP server in the field.

b) Disable the Optimize for low bandwidth parameter to ensure that Cisco IP Communicator sends voice packets for all calls.

Note The following steps are required to enable Cisco IP Communicator to support the G.711 codec, which is the fallback codec for Cisco Unified CME. You can compensate for disabling the optimization parameter by using the codec command in ephone configuration mode to configure G.729 or another advanced codec as the preferred codec for Cisco IP Communicator. This helps to ensure that the codec for a VoIP (For example, SIP or H.323) dial-peer is supported by Cisco IP Communicator and can prevent audio problems caused by insufficient bandwidth.

- Right-click on the Cisco IP Communicator interface and choose **Preferences** > **Audio**.
- Uncheck the checkbox next to Optimize for low bandwidth.

Step 4 Wait for the Cisco IP Communicator application to connect and register to Cisco Unified CME.

Step 5 Test Cisco IP Communicator.
For more information, see Verify Cisco IP Communicator Support on SCCP Phone, on page 311.

Verify Cisco IP Communicator Support on SCCP Phone

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 softkeys in its configuration. Verify that these are correct.

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

Troubleshooting Cisco IP Communicator Support on SCCP Phone

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

Configure Secure IP Phone (IP-STE) on SCCP Phone

To configure an IP-STE phone on Cisco Unified CME, perform the following steps.

Restriction

- Detection or conversion between Network Transmission Equipment (NTE) and Session Signaling Event (SSE) is not supported.
- Transcoding or trans-compress rate support for different Voice Band Data (VBD) and Modem Relay (MR) media type is not supported.
- IP-STE supports only single-line calls, dual-line and octo-line calls are not supported.
- Speed-dial can only be configured manually on the IP-STE.

Before You Begin

Cisco Unified CME 8.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mac-address** [*mac-address*]
5. **type ip-ste**
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	**ephone** *phone-tag* **Example:** `Router(config)# ephone 6`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type **?** to display range.
Step 4	**mac-address** [*mac-address*] **Example:** `Router(config-ephone)# mac-address 2946.3f2.311`	Specifies the MAC address of the IP phone that is being configured.

	Command or Action	Purpose
Step 5	**type ip-ste** **Example:** `Router(config-ephone)# type ip-ste`	Specifies the type of phone.
Step 6	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Configure Phone Services XML File for Cisco Unified Wireless Phone 7926G

To configure the phone services XML file for Cisco Unified Wireless phone 7926G, perform the following steps:

Before You Begin

Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mac-address** [*mac-address*]
5. **type** *phone-type*
6. **button** *button-number*
7. **ephone-template** *template tag*
8. **service** [**phone** *parameter name parameter value*] | [**xml-config append** *phone_service xml filename*]
9. **telephony-service**
10. **cnf-file perphone**
11. **create cnf-files**
12. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode.
Step 4	**mac-address** [*mac-address*] **Example:** `Router(config-ephone)# mac-address 0001.2345.6789`	Specifies the MAC address of the IP phone that is being configured.
Step 5	**type** *phone-type* **Example:** `Router(config-ephone)# type 7926`	Specifies the type of phone that is being configured.
Step 6	**button** *button-number* **Example:** `Router(config-ephone)# button 1:1`	Creates a set of ephone-dns overlaid on a single button.
Step 7	**ephone-template** *template tag* **Example:** `Router(config)#ephone-template 5`	Enters ephone-template configuration mode to create an ephone template.
Step 8	**service** [**phone** *parameter name parameter value*] | [**xml-config append** *phone_service xml filename*] **Example:** `Router(config-ephone-template)#service xml-config append flash:7926_phone_services.xml`	Sets parameters for all IP phones that support the configured functionality and to which this template is applied. • *parameter name*—The parameter name is word and case-sensitive. See Cisco Unified CME Command Reference. • *phone_service xml filename*—Allows the addition of a phone services xml file.
Step 9	**telephony-service** **Example:** `Router(config)telephony-service`	Enters telephony-service configuration mode.
Step 10	**cnf-file perphone** **Example:** `(config-telephony)# cnf-file perphone`	Specifies that the system generates a separate configuration XML file for each IP phone. • Separate configuration files for each endpoint are required for security.

	Command or Action	Purpose
Step 11	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds XML configuration files required for SCCP phones.
Step 12	**end** **Example:** `Router(config-telephony)#end`	Returns to privileged EXEC mode.

Configure Phones to Make Basic Call

Configure Auto Registration for SIP Phones

To configure automatic registration of SIP phones with the Cisco Unified CME system, perform the following steps.

Restriction

- The DNs assigned to auto registered phones cannot be configured as shared line DNs.
- Only Cisco Unified 7800 and 8800 series phones are supported with auto registration.

Before You Begin

- Cisco CME 11.5 or a later version.
- It is recommended that administrators choose different DN ranges for manually configured and auto configured phones.
- It is mandatory that **password** is configured before DN range (**auto-assign**) while registering SIP phones using auto registration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **auto-register**
5. **password** *string*
6. **auto-assign** *First DN number to Last DN number*
7. **service-enable**
8. **template** *tag*
9. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 4	**auto-register** **Example:** `Router(config-register-global)# auto-register`	Enters auto registration mode for SIP phones registering with Unified CME.
Step 5	**password** *string* **Example:** `Router(config-voice-auto-register)# password cisco`	Configures the default password for SIP phones that auto register. • *string*—Configures the mandatory word string that administrator provides for auto registration of phones on Unified CME.
Step 6	**auto-assign** *First DN number to Last DN number* **Example:** `Router(config-voice-auto-register)# auto-assign 1 to 10`	Configures the range of directory numbers for phones that auto register on Unified CME. • *First DN number to Last DN number*—Range is 1 to 4294967295.

	Command or Action	Purpose
Step 7	**service-enable** **Example:** `Router(config-voice-auto-register)# service-enable`	Enables the auto registration of SIP phones on Unified CME. Once auto-register command is entered, the service is enabled by default. To temporarily disable auto registration feature without losing DN and password configurations, use the no form of this command.
Step 8	**template** *tag* **Example:** `Router(config-voice-auto-register) template 10`	Configures a basic configuration template that supports all the configurations available on the voice register template. • It is mandatory that voice register template is configured with the same template tag. • *tag*—Range is 1 to 10.
Step 9	**end** **Example:** `Router(config-voice-auto-register)# end`	Exits to privileged EXEC mode.

Configure a Mixed Shared Line

To configure a mixed shared line between Cisco Unified SIP IP and Cisco Unified SCCP IP phones, perform the following steps.

Restriction

- Cisco Unified SCCP trunk-dn is not supported.
- Mixed shared lines can only be configured on one of several common directory numbers.
- Mixed shared lines are not supported in Cisco Unified SRST.

Before You Begin

Cisco Unified CME 9.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **shared-line** [**max-calls** *number-of-calls*]
6. **exit**
7. **ephone-dn** *dn-tag* [**dual-line** | **octo-line**]
8. **number** *number*
9. **shared-line sip**
10. **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 register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn configuration mode. • *dn-tag*—Unique sequence number that identifies a particular directory number during configuration tasks. Range is 1 to 150 or the maximum defined by the **max-dn** command.
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 1001`	Associates a telephone or extension number with a Cisco Unified SIP IP phone in a Cisco Unified CME system. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally, the string is composed of digits, but the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number.
Step 5	**shared-line** [**max-calls** *number-of-calls*] **Example:** `Router(config-register-dn)# shared-line max-calls 4`	Creates a directory number to be shared by multiple Cisco Unified SIP IP phones. • **max-calls** *number-of-calls*—(Optional) Maximum number of active calls allowed on the shared line. Range: 2 to 16. Default: 2.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-register-dn)# exit`	Exits voice register dn configuration mode.
Step 7	**ephone-dn** *dn-tag* [**dual-line** | **octo-line**] **Example:** `Router(config)# ephone-dn 1 octo-line`	Enters ephone-dn configuration mode to configure a directory number for an IP phone line. • *dn-tag*—Unique number that identifies an ephone-dn during configuration tasks. Range is 1 to the number set by the **max-dn** command. • **dual-line**—(Optional) Enables two calls per directory number. • **octo-line**—(Optional) Enables eight calls per directory number.
Step 8	**number** *number* **Example:** `Router(config-ephone-dn)# number 1001`	Associates a telephone or extension number with this ephone-dn. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally, the string is composed of digits, but the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number.
Step 9	**shared-line sip** **Example:** `Router(config-ephone-dn)# shared-line sip`	Adds an ephone-dn as a member of a shared directory number in the database of the Shared-Line Service Module for a mixed shared line between Cisco Unified SIP and Cisco Unified SCCP IP phones.
Step 10	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.

Troubleshooting Tips for Mixed Shared Line

Use the **debug ephone shared-line-mixed** command to display debugging information about mixed shared lines.

Configure the Maximum Number of Calls on SCCP Phone

To configure the maximum number of calls on a Cisco Unified SCCP IP phone in Cisco Unified CME 9.0, perform the following steps.

Before You Begin

- Cisco Unified CME 9.0 and later versions.
- Correct firmware, 9.2(1) or a later version, is installed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line** | **octo-line**]
4. **number** *number*
5. **exit**
6. **ephone** *phone-tag*
7. **mac-address** *mac-address*
8. **type** *phone-type*
9. **busy-trigger-per-button** *number-of-calls*
10. **max-calls-per-button** *number-of-calls*
11. **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-dn** *dn-tag* [**dual-line** | **octo-line**] **Example:** `Router(config)# ephone-dn 6 octo-line`	Enters ephone-dn configuration mode to configure a directory number for an IP phone line. • *dn-tag*—Unique number that identifies an ephone-dn during configuration tasks. Range is 1 to the number set by the **max-dn** command. • **dual-line**—(Optional) Enables two calls per directory number. • **octo-line**—(Optional) Enables eight calls per directory number.
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 1007`	Associates a telephone or extension number with an ephone-dn in a Cisco Unified CME. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally the string is composed of digits, but

	Command or Action	Purpose
		the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number. One or more periods (.) can be used as wildcard characters.
Step 5	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 98`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type **?** to display range.
Step 7	**mac-address** *mac-address* **Example:** `Router(config-ephone)# mac-address ABCD.1234.56EF`	Associates the MAC address of a Cisco IP phone with an ephone configuration in a Cisco Unified CME. • *mac-address*—Identifying MAC address of an IP phone.
Step 8	**type** *phone-type* **Example:** `Router(config-ephone)# type 8941`	Assigns a phone type to an SCCP phone.
Step 9	**busy-trigger-per-button** *number-of-calls* **Example:** `Router(config-ephone)# busy-trigger-per-button 6`	Sets the maximum number of calls allowed on an octo-line directory number before activating Call Forward Busy or a busy tone. • *number-of-calls*—Maximum number of calls. Range: 1 to 8. Default: 0 (disabled).
Step 10	**max-calls-per-button** *number-of-calls* **Example:** `Router(config-ephone)# max-calls-per-button 4`	Sets the maximum number of calls allowed on an octo-line directory number on an SCCP phone. • *number-of-calls*—Maximum number of calls. Range: 1 to 8. Default: 8.
Step 11	**end** **Example:** `Router(config-ephone)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure the Busy Trigger Limit on SIP Phone

To configure the busy trigger limit on a Cisco Unified SIP IP phone in Cisco Unified CME 9.0, perform the following steps.

Restriction You cannot configure the maximum number of calls per line. The phone controls the maximum number of outgoing calls.

Table 18: Maximum Number of Incoming and Outgoing Calls , on page 322 shows the maximum number of outgoing calls allowed by a phone and the maximum number of incoming calls that can be configured using the **busy-trigger-per-button** command for Cisco Unified 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones in Cisco Unified CME 9.0.

Table 18: Maximum Number of Incoming and Outgoing Calls

Cisco Unified SIP IP Phones	Maximum Number of Outgoing Calls (Controlled by Phones)	Maximum Number of Incoming Calls Before Busy Tone (Configurable)
6921	12	12
6941	24	24
6945	24	24
6961	72	72
8941	24	24
8945	24	24

Before You Begin

- Cisco Unified CME 9.0 and later versions.
- Correct firmware is installed:
    - 9.2(1) or a later version for Cisco Unified 6921, 6941, 6945 and 6961 SIP IP phones.
    - 9.2(2) or a later version for Cisco Unified 8941 and 8945 SIP IP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **type** *phone-type*
5. **busy-trigger-per-button** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 20`	Enters voice register pool configuration mode and creates a pool configuration for a SIP IP phone in Cisco Unified CME. *pool-tag*—Unique number assigned to the pool. Range is 1 to 100. **Note** For Cisco Unified CME systems, the upper limit for this argument is defined by the **max-pool** command.
Step 4	**type** *phone-type* **Example:** `Router(config-register-pool)# type 6921`	Defines a phone type for a SIP phone.
Step 5	**busy-trigger-per-button** *number* **Example:** `Router(config-register-pool)# busy-trigger-per-button 25`	Sets the maximum number of calls allowed on a SIP directory number before activating Call Forward Busy or a busy tone. • *number*—Maximum number of calls. Range: 1 to the maximum number of incoming calls listed in Step 6. The default values are 1 for the Cisco Unified 6921, 6941, 6945, and 6961 SIP IP phones and 2 for the Cisco Unified 8941 and 8945 SIP IP phones.
Step 6	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure KEMs on SIP Phones

To configure KEMs for Cisco Unified 8961, 9951, or 9971 SIP IP phones, perform the following steps.

Before You Begin

Cisco Unified CME 9.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **type** *phone-type* [**addon 1 CKEM** [**2 CKEM** [**3 CKEM**]]]

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 register pool** *pool-tag* **Example:** `Router(config)# voice register pool 29`	Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME. • *pool-tag*—Unique number assigned to the pool. Range is 1 to 100. **Note** For Cisco Unified CME systems, the upper limit for this argument is defined by the **max-pool** command.
Step 4	**type** *phone-type* [**addon 1 CKEM** [**2 CKEM** [**3 CKEM**]]] **Example:** `Router(config-register-pool)# type 9971 addon 1 CKEM 2 CKEM 3 CKEM`	Defines a phone type for a Cisco Unified SIP IP phone. The following keywords increase the number of speed-dial, busy-lamp-field, and directory number keys that can be configured: • **addon 1 CKEM—**(Optional) Tells the router that a Cisco SIP IP Phone CKEM 36-Button Line Expansion Module is being added to this Cisco Unified SIP IP Phone. **Note** This option is available to Cisco Unified 8961, 9951, and 9971 SIP IP phones only. • **2 CKEM** (Optional)—Tells the router that a second Cisco SIP IP Phone CKEM 36-Button Line Expansion Module is being added to this Cisco Unified SIP IP Phone.

	Command or Action	Purpose
		Note This option is available to Cisco Unified 9951 and 9971 SIP IP phones only. • **3 CKEM**—(Optional) Tells the router that a third Cisco SIP IP Phone CKEM 36-Button Line Expansion Module is being added to this Cisco Unified SIP IP Phone. **Note** This option is available to Cisco Unified 9971 SIP IP phones only.

Provision SIP Phones to Use the Fast-Track Configuration Approach

To provision the Cisco Unified SIP IP phones using the fast-track configuration approach, perform the following steps.

Restriction When a new Cisco Unified SIP IP phone is configured on Cisco Unified CME using the fast-track configuration approach, and the Cisco Unified CME is upgraded to a later version that supports the new phone type, the fast-track configuration pertaining to that SIP IP phone is removed automatically.

Before You Begin

You require Cisco Unified CME Release 10 or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool-type** *pool-type*
4. **addons** *max-addons*
5. **description** *string*
6. **gsm-support**
7. **num-lines** *max-lines*
8. **Phoneload-support**
9. **reference-pooltype** *phone-type*
10. **telnet-support**
11. **transport** {**udp** | **TCP**}
12. **Xml-config** {**maxNumCalls** | **busyTrigger** | **custom**}
13. **exit**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**voice register pool-type** *pool-type* **Example:** `Router(config)# voice register pool-type 9900`	Enters the voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME. If the new phone type is an existing phone that is supported on Cisco Unified CME release, you get the following error message: `ERROR: 8945 is built-in phonemodel, cannot be changed`
Step 4	**addons** *max-addons* **Example:** `Router(config-register-pooltype)# addons 3`	Defines the maximum number of add-on modules supported in Cisco Unified SIP IP phones. • *max-addons*—The maximum allowed value is 3. The configured add-on modules can be used while defining the pool for the new SIP phone model using the existing **type** command as shown below: **type <phone-type>** `[addon 1 module-type [2 module-type]]`
Step 5	**description** *string* **Example:** `Router(config-register-pooltype)# description TEST PHON`	Defines the description string for the new phone type.
Step 6	**gsm-support** **Example:** `Router(config-register-pooltype)# gsm-support`	Defines phone support for Global System for Mobile Communications (GSM) support.
Step 7	**num-lines** *max-lines* **Example:** `Router(config-register-pooltype)# num-lines 12`	Defines the maximum number of lines supported by the new phone. • *max-lines*—If this parameter is not configured, the default value 1 is used.

	Command or Action	Purpose
Step 8	**Phoneload-support** **Example:** `Router(config-register-pooltype)# Phoneload-support`	Defines phone support for firmware download from Cisco Unified CME. You can use the load command in the voice register global mode to configure the corresponding phone load for the new phone type if it supports phone load.

Step 9	**reference-pooltype** *phone-type*
	
	Example:
	`voice register pool-type 7821?`
	`description Cisco IP Phone 7821`
	`reference-pooltype 6921`
		Defines the nearest phone family from which the SIP IP phone in fast-track mode will inherit the properties.
		
		• *phone-type*—Unique number that represents the phone model.
		
		Default There is no reference point to inherit the properties.

Step 10	**telnet-support** **Example:** `Router(config-register-pooltype)# telnet-support`	Defines phone support for Telnet access.
Step 11	**transport** {**udp** | **TCP**} **Example:** `Router(config-register-pooltype)# transport TCp`	Defines the default transport type supported by the new phone. If this parameter is not configured, UDP is used as the default value. The **session-transport** command configured at the voice register pool takes priority over this configuration.

Step 12	**Xml-config** {**maxNumCalls** | **busyTrigger** | **custom**}
	
	Example:
	`Router(config-register-pooltype)#xml-config busyTrigger 2`
	`Router(config-register-pooltype)#xml-config maxNumCalls 4`
	`Router(config-register-pooltype)#xml-config custom <test>1</test>`
		Defines the phone-specific XML tags to be used in the configuration file.
		
		• **maxNumCalls—**Defines the maximum number of calls allowed per line.
		
		• **busyTrigger—**Defines the number of calls that triggers Call Forward Busy per line on the SIP phone.
		
		• **custom—**Defines custom XML tags which can be appended at the end of the phone specific CNF file.
		
		These parameters are used while generating the configuration profile file. CUCME does not use these configuration values for any other purpose.

Step 13	**exit** **Example:** `Router(config-register-pooltype)# exit`	Exits the voice register-pooltype configuration mode.
Step 14	**end** **Example:** `Router(config)# end`	Exits the privileged EXEC configuration mode.

SIP Phone Models Validated for CME using Fast-track Configuration

For information on the SIP phone models validated for Cisco Unified CME using fast-track configuration, see Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

Configuration Examples for Making Basic Calls

This section contains the following examples of the required Cisco Unified CME configurations with some of the additional options that are discussed in other modules.

Example for Configuring SCCP Phones for Making Basic Calls

The following is a sample output of the **show running-config** command, showing how an SCCP phone is configured to make basic calls:

```
Router# show running-config

version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CME40
!
boot-start-marker
boot-end-marker
!
logging buffered 2000000 debugging
!
no aaa new-model
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
no network-clock-participate slot 2
voice-card 0
 no dspfarm
 dsp services dspfarm
!
voice-card 2
 dspfarm
!
no ip source-route
ip cef
!
!
!
ip domain name cisco.com
ip multicast-routing
```

```
!
!
ftp-server enable
ftp-server topdir flash:
isdn switch-type primary-5ess
!
!
!
voice service voip
 allow-connections h323 to sip
 allow-connections sip to h323
 no supplementary-service h450.2
 no supplementary-service h450.3
 h323
  call start slow
!
!
!
controller T1 2/0/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2/0/1
 framing esf
 linecode b8zs
!
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip pim dense-mode
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
!
interface Service-Engine1/0
 ip unnumbered GigabitEthernet0/0
 service-module ip address 192.168.1.2 255.255.255.0
 service-module ip default-gateway 192.168.1.1
!
interface Serial2/0/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 isdn map address ^.* plan unknown type international
 no cdp enable
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.2 255.255.255.255 Service-Engine1/0
ip route 192.168.2.253 255.255.255.255 10.2.0.1
ip route 192.168.3.254 255.255.255.255 10.2.0.1
!
!
ip http server
ip http authentication local
no ip http secure-server
ip http path flash:
!
!
!
!
tftp-server flash:P00307020300.loads
tftp-server flash:P00307020300.sb2
tftp-server flash:P00307020300.sbn
!
control-plane
!
!
!
voice-port 2/0/0:23
```

```
!
!
!
sccp local GigabitEthernet0/0
sccp ccm 192.168.1.1 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register MTP0013c49a0cd0
 keepalive retries 5
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec gsmfr
 codec g729r8
 maximum sessions 90
 associate application SCCP
!
!
dial-peer voice 9000 voip
 mailbox-selection last-redirect-num
 destination-pattern 78..
 session protocol sipv2
 session target ipv4:192.168.1.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 2 pots
 incoming called-number .
 direct-inward-dial
 port 2/0/0:23
 forward-digits all
!
dial-peer voice 1 pots
 destination-pattern 9[2-9]......
 port 2/0/0:23
 forward-digits 8
!
dial-peer voice 3 pots
 destination-pattern 91[2-9]..[2-9]......
 port 2/0/0:23
 forward-digits 12!
!
gateway
 timer receive-rtp 1200
!
!
telephony-service
 load 7960-7940 P00307020300
 max-ephones 100
 max-dn 300
 ip source-address 192.168.1.1 port 2000
 system message CCME 4.0
 sdspfarm units 1
 sdspfarm transcode sessions 128
 sdspfarm tag 1 MTP0013c49a0cd0
 voicemail 7800
 max-conferences 24 gain -6
 call-forward pattern .T
 moh music-on-hold.au
 multicast moh 239.1.1.1 port 2000
 web admin system name admin password sjdfg
 transfer-system full-consult
 transfer-pattern .T
 secondary-dialtone 9
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
```

```
ephone-dn-template  1
!
!
ephone-template  1
 keep-conference endcall local-only
 codec g729r8 dspfarm-assist
!
!
ephone-template  2
!
!
ephone-dn  1
 number 6001
 call-forward busy 7800
 call-forward noan 7800 timeout 10
!
!
ephone-dn  2
 number 6002
 call-forward busy 7800
 call-forward noan 7800 timeout 10
!
!
ephone-dn  10
 number 6013
 paging ip 239.1.1.1 port 2000
!
!
ephone-dn  20
 number 8000....
 mwi on
!
!
ephone-dn  21
 number 8001....
 mwi off
!
!
!
!
ephone  1
 device-security-mode none
 username "user1"
 mac-address 002D.264E.54FA
 codec g729r8 dspfarm-assist
 type 7970
 button  1:1
!
!
!
ephone  2
 device-security-mode none
 username "user2"
 mac-address 001C.821C.ED23
 type 7960
 button  1:2
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output all
line 258
 no activation-character
 no exec
 transport preferred none
```

```
 transport input all
 transport output all
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password sgpxw
 login
!
scheduler allocate 20000 1000
ntp server 192.168.224.18
!
!
end
```

Example for Configuring SIP Phones for Making Basic Calls

The following is a configuration example for SIP phones running on Cisco Unified CME:

```
voice service voip
 allow-connections sip to sip
 sip
 registrar server expires max 600 min 60
!
voice class codec 1
 codec preference 1 g711ulaw
!
voice hunt-group 1 parallel
 final 8000
 list 2000,1000,2101
 timeout 20
 pilot 9000
!
voice hunt-group 2 sequential
 final 1000
 list 2000,2300
 timeout 25
 pilot 9100 secondary 9200
!
voice hunt-group 3 peer
 final 2300
 list 2100,2200,2101,2201
 timeout 15
 hops 3
 pilot 9300
 preference 5
!
voice hunt-group 4 longest-idle
 final 2000
 list 2300,2100,2201,2101,2200
 timeout 15
 hops 5
 pilot 9400 secondary 9444
 preference 5 secondary 9
!
voice register global
 mode cme
!
 external-ring bellcore-dr3
!
voice register dn 1
 number 2300
 mwi
!
voice register dn 2
 number 2200
 call-forward b2bua all 1000
 call-forward b2bua mailbox 2200
 mwi
!
voice register dn 3
```

```
 number 2201
 after-hour exempt
!
voice register dn 4
 number 2100
 call-forward b2bua busy 2000
 mwi

voice register dn 5
 number 2101
 mwi

voice register dn 76
 number 2525
 call-forward b2bua unreachable 2300
 mwi
!
voice register template 1
!
voice register template 2
 no conference enable
 voicemail 7788 timeout 5
!
voice register pool 1
 id mac 000D.ED22.EDFE
 type 7960
 number 1 dn 1
 template 1
 preference 1
 no call-waiting
 codec g711alaw
!
voice register pool 2
 id mac 000D.ED23.CBA0
 type 7960
 number 1 dn 2
 number 2 dn 2
 template 1
 preference 1
!
 dtmf-relay rtp-nte
 speed-dial 3 2001
 speed-dial 4 2201
!
voice register pool 3
 id mac 0030.94C3.053E
 type 7960
 number 1 dn 3
 number 3 dn 3
 template 2
!
voice register pool 5
 id mac 0012.019B.3FD8
 type ATA
 number 1 dn 5
 preference 1
 dtmf-relay rtp-nte
 codec g711alaw
!
voice register pool 6
 id mac 0012.019B.3E88
 type ATA
 number 1 dn 6
 number 2 dn 7
 template 2
 dtmf-relay-rtp-nte
 call-forward b2bua all 7778
!
voice register pool 7
!
voice register pool 8
 id mac 0006.D737.CC42
 type 7940
```

```
 number 1 dn 8
 template 2
 preference 1
 codec g711alaw
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer voice 100 pots
 destination-pattern 2000
 port 1/0/0
!
dial-peer voice 101 pots
 destination-pattern 2010
 port 1/0/1
!
dial-peer voice 1001 voip
 preference 1
 destination-pattern 1...
 session protocol sipv2
 session target ipv4:10.15.6.13
 codec g711ulaw
!
sip-ua
 mwi-server ipv4:1.15.6.200 expires 3600 port 5060 transport udp
!
telephony-service
 load 7960-7940 P0S3-07-2-00
 max-ephones 24
 max-dn 96
 ip source-address 10.15.6.112 port 2000
 create cnf-files version-stamp Aug 24 2004 00:00:00
 max-conferences 8
 after-hours block pattern 1 1...
 after-hours day Mon 17:00 07:00
```

Example for Disabling a Bulk Registration for a SIP Phone

The following example shows that all phone numbers that match the pattern “408555..” can register with the SIP proxy server (IP address 1.5.49.240) except directory number 1, number “4085550101,” for which bulk registration is disabled:

```
voice register global
 mode cme
 bulk 408555….
!
voice register dn 1
 number 4085550101
 no-reg
sip-ua
 registrar ipv4:1.5.49.240
```

Example for Configuring a Mixed Shared Line on a Second Common Directory Number

The following example shows how configuring a mixed shared line on a second common directory number is rejected:

```
Router(config)#ephone-dn 14 octo-line
Router(config-ephone-dn)#number 2502
Router(config-ephone-dn)#shared-line sip

Router(config)#ephone-dn 20 octo-line
```

```
Router(config-ephone-dn)#number 2502
Router(config-ephone-dn)#shared-line sip
DN number already exists in the shared line database
```

Example for Cisco ATA

The following example shows the configuration for two analog phones using a single Cisco ATA with MAC address 000F.F758.E70E. The analog phone attached to the first port uses the MAC address of the Cisco ATA. The analog phone attached to the second port uses a modified version of the Cisco ATA's MAC address; the first two hexadecimal numbers are removed and 01 is appended to the end.

```
telephony-service
 conference hardware
 load ATA ATA030203SCCP051201A.zup
!
ephone-dn  80  dual-line
 number 8080
!
ephone-dn  81  dual-line
 number 8081
!
ephone  30
 mac-address 000F.F758.E70E
 type ata
 button  1:80
!
ephone  31
 mac-address 0FF7.58E7.0E01
 type ata
 button  1:81
```

Example for SCCP Analog Phone

The following partial sample output from a Cisco Unified CME configuration sets transfer type to full-blind and sets the voice-mail extension to 5200. Ephone-dn 10 has the extension 4443 and is assigned to Tommy; that number and name will be used for caller-ID displays. The description field under ephone-dn is used to indicate that this ephone-dn is on the Cisco VG224 voice gateway at port 1/3. Extension 4443 is assigned to ephone 7, which is an analog phone type with 10 speed-dial numbers.

```
CME_Router# show running-config
.
.
.
telephony-service
 load 7910 P00403020214
 load 7960-7940 P00305000301
 load 7905 CP79050101SCCP030530B31
 max-ephones 60
 max-dn 60
 ip source-address 10.8.1.2 port 2000
 auto assign 1 to 60
 create cnf-files version-stamp 7960 Sep 28 2004 17:23:02
 voicemail 5200
 mwi relay
 mwi expires 99999
 max-conferences 8 gain -6
 web admin system name cisco password lab
 web admin customer name ac2 password cisco
 dn-webedit
 time-webedit
 transfer-system full-blind
 transfer-pattern 6...
 transfer-pattern 5...
!
```

```
!
ephone-dn  10  dual-line
 number 4443 secondary 9191114443
 pickup-group 5
 description vg224-1/3
 name tommy
!
ephone  7
 mac-address C863.9018.0402
 speed-dial 1 4445
 speed-dial 2 4445
 speed-dial 3 4442
 speed-dial 4 4441
 speed-dial 5 6666
 speed-dial 6 1111
 speed-dial 7 1112
 speed-dial 8 9191114441
 speed-dial 9 9191114442
 speed-dial 10 9191114442
 type anl
 button  1:10
```

Example for Remote Teleworker Phones

The following example shows the configuration for ephone 270, a remote teleworker phone with its codec set to G.729r8. The **dspfarm-assist** keyword is used to ensure that calls from this phone will use DSP resources to maintain the G.729r8 codec when calls would normally be switched to a G.711 codec.

```
ephone 270
 button 1:36
 mtp
 codec g729r8 dspfarm-assist
 description teleworker remote phone
```

Example for Secure IP Phone (IP-STE)

The following example shows the configuration for Secure IP Phone IP-STE. IP-STE is the phone type required to configure a secure phone.

```
ephone-dn  1
 number 3001
...
ephone  9
 mac-address 0004.E2B9.1AD1
 max-calls-per-button 1
 type IP-STE
 button  1:1 2:2 3:3 4:4
```

Example for Configuring Phone Services XML File for Cisco Unified Wireless Phone 7926G

The following example shows phone type 7926 configured in ephone 1 and service xml-config file configured in ephone template 1:

```
!
!
!
telephony-service
 max-ephones 58
 max-dn 192
 ip source-address 1.4.206.105 port 2000
```

```
 cnf-file perphone
 create cnf-files
!
ephone-template 1
 service xml-config append flash:7926_phone_services.xml
!
ephone-dn  1 octo-line
  number 1001
!
ephone  1
  mac-address AAAA.BBBB.CCCC
  ephone-template 1
  type 7926
  button 1:1
!
```

Example for Monitoring the Status of Key Expansion Modules

Show commands are used to monitor the status and other details of Key Expansion Modules (KEMs).

The following example demonstrates how the **show voice register all** command displays KEM details with all the Cisco Unified CME configurations and registration information:

```
show voice register all
VOICE REGISTER GLOBAL
=====================
CONFIG [Version=9.1]
========================
............
Pool Tag 5
Config:
  Mac address is B4A4.E328.4698
  Type is 9971 addon 1 CKEM
  Number list 1 : DN 2
  Number list 2 : DN 3
  Proxy Ip address is 0.0.0.0
  DTMF Relay is disabled
  Call Waiting is enabled
  DnD is disabled
  Video is enabled
  Camera is enabled
  Busy trigger per button value is 0
  keep-conference is enabled
  registration expires timer max is 200 and min is 60
  kpml signal is enabled
  Lpcor Type is none
```

The following example demonstrates how the **show voice register pool type** command displays all the phones configured with add-on KEMs in Cisco Unified CME:

```
Router# show voice register pool type CKEM
Pool ID              IP Address      Ln DN  Number               State
==== =============== =============== == === ==================== ============
4    B4A4.E328.4698  9.45.31.111     1  4   5589$                REGISTERED
```

The following example demonstrates how the show voice register pool type summary command displays all the SIP phones (both registered and unregistered) configured with add-on KEMs in Cisco Unified CME:

```
Router# show voice register pool type summary
Phone Type    Configured    Registered    Unregistered
==========    ==========    ==========    ============
Unknown type     2             0             2
    7821          1             0             1
    9951         1             1             0
    DX650        1              0             1
======================================================
```

```
Total Phones      5              1                 4
======================================================
```

Cisco IOS Commands for Monitoring and Maintaining Cisco Unified CME

To monitor and maintain Cisco Unified Communications Manager Express (CME), use the following commands in privileged EXEC mode.

Command	Purpose
`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 CME Router.
`Router#` **show call-manager-fallback dial-peer**	Displays the output of the dial peers of the Cisco Unified CME 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 dial-peer voice summary**	Displays a summary of all voice dial peers.
`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 summary brief**	Displays a brief summary of all Cisco Unified SCCP phones.
`Router#` **show ephone summary types**	Displays a summary of all types of Cisco Unified SCCP phones.
`Router#` **show ephone registered summary**	Displays a summary of all registered Cisco Unified SCCP phones.
`Router#` **show ephone unregistered summary**	Displays a summary of all unregistered Cisco Unified SCCP phones.

Command	Purpose
`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.
`Router#` **show running-config**	Displays the configuration.
`Router #` **show sip-ua status registrar**	Display SIP registrar clients.
`Router#` **show voice port summary**	Displays a summary of all voice ports.
`Router #` **show voice register all**	Displays all SIP SRST configurations , SIP phone registrations and dial peer info.
`Router #` **show voice register global**	Displays voice register global config.
`Router #` **show voice register pool all**	Displays all config SIP phone voice register pool detail info.
`Router #` **show voice register pool type summary**	Displays a summary of all registered and unregistered Cisco SIP Phones.
`Router #` **show voice register pool <tag>**	Displays specific SIP phone voice register pool detail info.
`Router #` **show voice register dial-peers**	Displays SIP-CME created dial peer.
`Router #` **show voice register dn all**	Displays all config voice register dn detail info.
`Router #` **show voice register dn <tag>**	Displays specific voice register dn detail info.

Example for Fast-Track Configuration Approach

The following example shows how to enable the new Cisco Unified 9900 SIP IP phone to inherit the properties of the Cisco Unified SIP IP phone 9951 and overwrite some of the phone's properties:

```
voice register pool-type 9900
 reference-pooltype  9951
 description  SIP Phone 9900 addon module
```

```
  num-lines  24
 addons 3
   no phoneload-support
 xml-config custom "custom-sftp"1"/custom-sftp"

voice register pool 1
 type 9900 addon 1 CKEM 2 CKEM 3 CKEM
 id mac 1234.4567.7891
voice register global
 mode cme
 load 9900 P0S3-06-0-00
```

The following example shows how to inherit the existing properties of a reference phone type (Cisco Unified SIP IP phone 6921) using the fast-track configuration approach.

```
voice register pooltype 6922
 reference-pooltype 6921
 device-name  "SIP Phone 6922"

voice register pool 11
 type 6922
 id mac 1234.4567.7890
```

Where To Go Next

To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see Select Button Layout for a Cisco Unified SCCP IP Phone 7931G, on page 1453.

After configuring phones in Cisco Unified CME to make basic calls, you are ready to generate configuration files for the phones to be connected to your router. See Generate Configuration Files for Phones, on page 388.

Feature Information for Configuring Phones to Make Basic Calls

Caution The Interactive Voice Response (IVR) media prompts feature is only available on the IAD2435 when running IOS version 15.0(1)M or later.

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

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

Table 19: Feature Information for Basic Call Features

Feature Name	Cisco Unified CME Versions	Feature Information
KEM Support for Cisco Unified 8961, 9951, and 9971 SIP IP Phones	9.1	Increases line key and feature key appearances, speed dials, or programmable buttons on Cisco Unified SIP IP phones.

Feature Name	Cisco Unified CME Versions	Feature Information
Cisco ATA-187	9.0	Supports T.38 fax relay and fax pass-through on Cisco ATA-187.
Cisco Unified SIP IP Phones		Adds SIP support for the following phone types: • Cisco Unified 6901 and 6911 IP Phones • Cisco Unified 6921, 6941, 6945, and 6961 IP Phones • Cisco Unified 8941 and 8945 IP Phones
Mixed Shared Lines		Allows Cisco Unified SIP and SCCP IP phones to share a common directory number.
Multiple Calls Per Line		Overcomes the limitation on the maximum number of calls per line.
Real-Time Transport Protocol Call Information Display Enhancement	8.8	Allows you to display information on active RTP calls using the **show ephone rtp connections** command. The output from this command provides an overview of all the connections in the system, narrowing the criteria for debugging pulse code modulation and Cisco Unified CME packets without a sniffer.
Support for Cisco Unified 3905 SIP IP Phones		Adds support for SIP phones connected to a Cisco Unified CME system.
Support for Cisco Unified 6945, 8941, and 8945 SCCP IP Phones		Adds support for SCCP phones connected to a Cisco Unified CME system.
Support for 7926G Wireless SCCP IP Phone	8.6	Added support for 7926G Wireless SCCP IP Phone.

Feature Name	Cisco Unified CME Versions	Feature Information
Secure IP Phones	8.0	Adds support for Secure IP Phone (IP-STE).
SIP Shared Lines	7.1	Adds support for nonexclusive shared lines on SIP phones.
Autoconfiguration for Cisco VG202, VG204, and VG224		Adds autoconfiguration for the Cisco VG202, VG204, and VG224 Analog Phone Gateway.
Ephone-Type Templates	7.0/4.3	Adds support for dynamically adding new phone types without upgrading Cisco IOS software.
Octo-Line Directory Numbers		Adds octo-line directory numbers that support up to eight active calls.
G.722 and iLBC Transcoding and Conferencing Support in Cisco Unified CME		Adds support for the G.722-64K and iLBC codecs.
Dial Plans for SIP Phones	4.1	Adds support for dial plans for SIP phones.
KPML		Adds support for KPML for SIP phones.
Session Transport Protocol		Adds selection for session-transport protocol for SIP phones.
Watch Mode		Provides Busy Lamp Field (BLF) notification on a line button that is configured for watch mode on one phone for all lines on another phone (watched phone) for which the watched directory number is the primary line.
Remote Teleworker Phones	4.0	Introduces support for teleworker remote phones.

Feature Name	Cisco Unified CME Versions	Feature Information
Analog Phones	4.0	Introduces support for analog phones with SCCP supplementary features using FXS ports on Cisco Integrated Services Routers.
	3.2.1	Introduces support for analog phones with SCCP supplementary features using FXS ports on a Cisco VG224 voice gateway.
	3.0	Introduces support for Cisco ATA 186 and Cisco ATA 188.
	1.0	Introduces support for analog phones in H.323 mode using FXS ports.
Cisco IP Communicator	4.0	Introduces support for Cisco IP Communicator.

Feature Name	Cisco Unified CME Versions	Feature Information
Direct FXO Trunk Lines	4.0	Adds enhancements to improve the keyswitch emulation behavior of PSTN lines in a Cisco Unified CME system, including the following: • Status monitoring of the FXO port on the line button of an IP phone. • Transfer recall if a transfer-to phone does not answer after a specified timeout. • Transfer-to button optimization to free up the private extension line on the transfer-to phone • Directory numbers for FXO lines can be configured for dual-line to support the FXO monitoring, transfer recall, and transfer-to button optimization features.
	3.2	Introduces direct FXO trunk line capability.
SIP Phones	3.4	Adds support for SIP phones connected to Cisco CME system.
Monitor Mode for Shared Lines	3.0	Provides a visible line status indicating whether the line is in-use or not.

CHAPTER 8

Create Phone Configurations Using Extension Assigner

Prerequisites for Extension Assigner

- Cisco Unified CME 11.6 or a later version for SIP phones.
- Cisco Unified CME 4.0(3) or a later version for SCCP phones.
- For Extension Assigner Synchronization, Cisco Unified CME 4.2(1) or a later version.
- The **auto-register-phone** command must be enabled (default) for SCCP phones, and **auto-register** must be enabled for SIP phones.
- DHCP must be configured. For configuration information, see Network Parameters.
- You have a valid Cisco.com account.
- You have access to a TFTP server for downloading files.

Restrictions for Extension Assigner

- The number of phones that you install cannot exceed the maximum number of phones supported by the router chassis. To find the maximum number of phones for a particular router and Cisco Unified CME version, see the appropriate Cisco Uniified CME Supported Firmware, Platforms, Memory, and Voice Products for your Cisco IOS release.
- For Extension Assigner Synchronization, automatic synchronization only applies to configuration changes made by Cisco Unified CME Extension Assigner.

Information About Extension Assigner

Extension Assigner Overview

From Cisco Unified CME Release 11.6 onwards, Extension Assigner feature is supported for both SIP and SCCP phones. This feature enables installation technicians to assign extension numbers to Cisco Unified CME phones without administrative access to the server, typically during the installation of new phones or the replacement of broken phones. However, before an installation technician can use this feature, the system administrator must first configure Cisco Unified CME to allow specific extensions to be assigned. The system administrator must also provide the installation technician with the information necessary for assigning extension numbers to phones. The installation technician can then assign extension numbers to phones with access to only the phones themselves and with no further intervention from the administrator.

To configure this feature, tasks must be performed on the Cisco router by an administrator and onsite by installation technicians.

Procedure for System Administrators

Before an installation technician can assign new extension numbers to phones, you must complete the following tasks:

1. Determine which extension numbers will be assigned to the new phones and plan your configuration.
2. Download the appropriate Tcl script and associated audio prompt files and place them in the correct directory.
3. Configure the Cisco Unified CME router to:
    - Configure and load the appropriate Tcl script.
    - Specify the extension that the installation technician calls to assign extension numbers.
    - Optionally specify whether the extension used to assign extension numbers is dialed automatically.
    - Specify the password that the installation technician enters to assign extension numbers.
    - Configure the extension assigner feature.
    - Configure ephone-dns with temporary extension numbers (applicable only for SCCP phones).
    - Configure ephone-dns and voice register dns with the extension numbers that the installation technician can assign to phones.

- Configure ephones and voice register pools with temporary MAC addresses for each phone that will be assigned an extension number by the installation technician.
- Optionally configure the router to automatically save your configuration.

Note All phone configurations such as dn and pool that are generated as part of the auto registration process are persistent configurations(If the command **background save interval** is configured under telephony-service). These phone configurations are available on Unified CME even after an event of router reload.

4 Provide the installation technician with the information needed to assign extension numbers to the new phones.

Before you can configure this feature, you must understand how the extension assigner application works and what information the installation technician needs to assign extension numbers to phones.

Other information you must provide to the installation technician involves the tasks that the installation technician must perform. These tasks include:

- Dialing a configurable extension number to access the extension assigner application.
- Entering a configurable password.
- Entering a tag (provision-tag for SIP phones, and ephone-tag or provision-tag for SCCP phones) that identifies the extension number that will be assigned to the phone.

Therefore, you must make the following decisions:

- Which extension number must be dialed to access the extension assigner application.
- Whether the number is dialed automatically when a phone goes off hook.
- What password the installation technician must enter to access the extension assigner application.
- What type of tag (provision-tag for SIP phones, and ephone-tag or provision-tag for SCCP phones) numbers to use to identify the extension number to assign to the phone.
- What specific tag numbers to use to identify the extension number to assign to the phone.

The first three decisions are straightforward, but the last two tag number decisions require some knowledge of how the extension assigner feature works.

This feature is implemented using a Tcl script and audio files. To run this script, the installation technician plugs in the phone, waits for a random extension number to be automatically assigned, and dials a specified extension assigner number to invoke the extension assigner service.

After the phones have registered and received their temporary extension numbers, the installation technician can access extension assigner and enter a tag number. This tag number is used to identify the extension number and must match either an ephone tag (only for SCCP phones) or a similar new tag called the provision-tag (applicable to both SIP and SCCP phones).

For SCCP phones, you must decide on which tag you want to use before you configure your ephone and ephone-dn entries.

The advantage of using the provision-tag is that you can make it easier for the installation technician to assign extension numbers because you can configure the tag to match the primary extension number or some other unique identifier for the phone, such as a jack number. We recommend you to configure provision-tag same as the primary extension number.

The disadvantage is that you configure an additional keyword for each ephone entry, as shown in the following example:

```
ephone 1
 provision-tag 9001
 mac-address 02EA.EAEA.0001
 button 1:1

voice register pool 1
 provision-tag 1001
 mac-address 02EA.EAEA.0001
 number 1 dn 101
```

For SCCP phones, if you decide to use the ephone tag, it requires less configuration. However, the installation technician enters an arbitrary tag number instead of the actual extension number when configuring a phone. This restriction is because the number of ephone tags that you can configure is limited by your license. For example, if you use the ephone tag and you have a 100-user license, the installation technician cannot enter 9001 for the tag because you can configure only ephone 1 to ephone 100.

Note that each ephone entry that you configure must also include a temporary MAC address. As shown in the above example, this address should begin with 02EA.EAEA and can end with any unique number. We strongly recommend that you can configure this unique number to match the ephone tag for SCCP phones.

For SCCP phones, you do not have to configure any ephone entries for the extension number that are randomly assigned. The auto assign feature automatically creates an ephone entry for each new phone when it registers. The auto assign feature then automatically assigns an ephone-dn entry if there is an available ephone-dn that has one of the tag numbers specified by the **auto assign** command. The resulting ephone pool configurations have the actual MAC address of the phone and a button with the first available ephone-dn designated for the auto assign feature. For more information, see Configure Temporary Extension Numbers for SCCP Phones That Use Extension Assigner, on page 361.

For SIP phones, you do not have to configure voice register pool or voice register dn. You need to configure auto-register command for automatic registration of SIP phones on Cisco Unified CME. For more information, see Configure Temporary Extension Numbers for SCCP Phones That Use Extension Assigner, on page 361.

Note For manually registered phones, ephone (or voice register pool) and ephone-dn (or voice register dn) are manually created.

As shown in the following example, you configure at least one ephone-dn for a temporary extension and specify which ephone-dns the autoassign feature will assign to the temporary ephone entries:

```
telephony-service
 auto assign 101 to 105
ephone-dn 101
 number 0001
```

When the installation technician assigns an extension number to a phone, the temporary MAC address is replaced by the actual MAC address and the ephone entry created by the auto register feature is deleted. The number of ephone-dns that you configure for the auto assign feature determines how many phones you can plug in at one time and get an automatically assigned extension. If you define four ephone-dns for auto assign and you plug in five phones, one phone will not get a temporary extension number until you assign an extension to one of the other four phones and reset the fifth phone. You are permitted to set the max-ephone value higher than the number of users and phones supported by your Cisco Unified CME phone licenses for the purpose of enrolling licensed phones using Extension Assigner.

In addition to configuring one ephone-dn for each temporary extension number that is assigned automatically, you also must configure an ephone-dn entry for each extension number that is assigned by the installation technician. For more details on configuring extension numbers that technicians can assign to SCCP phones, see Configure Extension Numbers That Installation Technicians Can Assign to SCCP Phones, on page 364.

For SIP Phones, the temporary MAC address is replaced by the actual MAC address and voice register pool entry created by the auto-register feature is deleted when the installation technician assigns an extension number to a phone. The number of voice register dns that you configure for the auto assign feature determines how many phones you can plug in at one time and get an automatically assigned extension. If you define four voice register dns for auto assign and you plug in five phones, one phone will not get a temporary extension number until you assign an extension to one of the other four phones and reset the fifth phone. You are permitted to set the max-pool value higher than the number of users and phones supported by your Cisco Unified CME phone licenses for the purpose of enrolling licensed phones using Extension Assigner. For more details on configuring extension numbers that technicians can assign to SIP phones, see Configure Extension Numbers That Installation Technicians Can Assign to SIP Phones, on page 366.

Note For SIP Phones, you need not create temporary dn if auto registration is used.

To complete the configuration, as shown in the following example, you must:

- Specify whether to use the ephone or the provision-tag number to identify the extension number to assign to the phone. Set this when the feature is enabled with the new **extension-assigner tag-type** command provided with this feature.
- Configure an ephone-dn for each temporary extension number that is assigned automatically.
- Configure an ephone-dn or voice register dn for each extension number that you want the installation technician to assign to a phone.
- Configure an ephone or voice register pool with a temporary MAC address for each phone that is assigned an extension number by the installation technician. Optionally, this ephone definition can include the new provision-tag. For SIP phones, it is necessary to have provision-tag information under voice register pool. For more information, see Configure Ephones with Temporary MAC Addresses, on page 368.

```
telephony-service
 extension-assigner tag-type provision-tag
 auto assign 101 to 105
ephone-dn 1 dual-line
 number 6001
ephone-dn 101
 number 0001
 label Temp-Line-not assigned yet
ephone 1
 provision-tag 6001
 mac-address 02EA.EAEA.0001
 button 1:1
***********************************

voice register pool 1
provision-tag 1001
mac-address 02EA.EAEA.0001
number 1 dn 101
```

Because you must configure two ephone-dns or voice register dns for each extension number that you want to assign, you may exceed your max-dn setting. You are permitted to set the max-dn value higher than the number allowed by your license for the purpose of enrolling licensed phones using extension assigner.

Assuming that your max-dn setting is set high enough, your max-ephone or max-pool setting determines how many phones you can plug in at one time. For example, if your max-ephone or max-pool setting is ten more than the number of phones to which you want to assign extension numbers, then you can plug in ten phones at a time. If you plug in eleven phones, one phone will not register or get a temporary extension number until you assign an extension to one of the first ten phones and reset the eleventh phone.

After you have configured your ephone or voice register pool, and ephone-dn or voice register dn entries, you can complete your router configuration by optionally configuring the router to automatically save your configuration. If the router configuration is not saved, any extension assignments made by the installation technician will be lost when the router is restarted. The alternative to this optional procedure is to have the installation technician connect to the router and enter the **write memory** command to save the router configuration.

The final task of the system administrator is to document the information that the installation technician needs to assign extension numbers to the new phones. You can also use this documentation as a guide when you configure Cisco Unified CME to implement this feature. This information includes:

- How many phones the installation technician can plug in at one time
- Which extension number to dial to access the extension assigner application
- Whether the number is dialed automatically when a phone goes off hook
- What password to enter to access the application
- Which tag numbers to enter to assign an extension to each phone

Note Because this feature is implemented using a Tcl script and audio files, you must place the script and associated audio prompt files in the correct directory. Do not edit this script; just configure Cisco Unified CME to load the appropriate script.

Extension Assigner in Mixed Deployment

From Cisco Unified CME release 11.6 onwards, extension assigner feature supports mixed deployment of SCCP and SIP phones. In a mixed deployment scenario, you sometimes have to migrate or replace an SCCP phone with a SIP phone or vice versa. The extension assigner functionality ensures a seamless migration experience in this scenario by letting you assign extension numbers to the new phone (irrespective of SIP or SCCP).

In mixed mode deployment, you can reassign any current extension number to a new phone. When you dial in to the extension assigner system to perform this task, you are redirected to the unassign menu. You need to unassign the current extension number so that it is no more assigned to any phone. After successfully unassigning the extension number, the call is disconnected. When you dial in to the extension assigner again, you can reassign the extension number to your new phone. For more information, see Reassign the Current Extension Number, on page 379.

Note You cannot unassign the extension number of a phone if it is in use. The phone has to be in idle or unregistered state.

Procedures for Installation Technicians

This feature is implemented using a Tcl script and audio prompt files that enable the installation technician to assign an extension number to a new Cisco Unified CME phone by performing the following procedure The system administrator provides the installation technician with all of the information required to perform this procedure.

Step 1 Plug in a specified number of new phones.

Step 2 Wait for the phones to be assigned temporary, random extension numbers.

Step 3 Dial a specified number to access the extension assigner application.

Step 4 Enter a specified password.

Step 5 Enter a tag that identifies an extension number and enables the installation technician to perform one of the following tasks:

- Assign a new extension number to a phone.
- Unassign the current extension number.
- Reassign an extension number.

Files Included in this Release

The app-cme-ea-2.0.0.0.tar or later archive file provided for the extension assigner feature includes a readme file, a Tcl script, and several audio prompt files. If you want to replace the audio files with files that use a language other than English, do not change the name of the files. The Tcl script is written to use only the following list of the filenames:

- app-cme-ea-2.0.0.0.tcl (script)
- en_cme_tag_assign_phone.au (audio file)
- en_cme_tag_assigned_to_phone.au (audio file)
- en_cme_tag_assigned_to_phone_idle.au (audio file)
- en_cme_tag_assigned_to_phone_inuse.au (audio file)
- en_cme_tag_assigned_to_phone_unreg.au (audio file)
- en_cme_tag_available.au (audio file)
- en_cme_tag_extension.au (audio file)
- en_cme_tag_invalid.au (audio file)
- en_cme_tag_unassign_phone.au (audio file)
- en_cme_tag_action_cancelled.au (audio file)
- en_cme_tag_assign_failed.au (audio file)

- en_cme_tag_assign_success.au (audio file)
- en_cme_tag_contact_admin.au (audio file)
- en_cme_tag_disconnect.au (audio file)
- en_cme_tag_ephone_tagid.au (audio file)
- en_cme_tag_invalid_password.au (audio file)
- en_cme_tag_invalidoption.au (audio file)
- en_cme_tag_noentry.au (audio file)
- en_cme_tag_password.au (audio file)
- en_cme_tag_unassign_failed.au (audio file)
- en_cme_tag_unassign_success.au (audio file)
- en_eight.au (audio file)
- en_five.au (audio file)
- en_four.au (audio file)
- en_nine.au (audio file)
- en_one.au (audio file)
- en_seven.au (audio file)
- en_six.au (audio file)
- en_three.au (audio file)
- en_two.au (audio file)
- en_zero.au (audio file)
- readme.txt

Extension Assigner Synchronization

Extension Assigner Synchronization enables the secondary backup router to automatically receive any changes made by Extension Assigner to ephone or voice register pool mac-addresses in the primary router. The synchronization is performed using the Cisco Unified CME XML interface. The Cisco Unified CME XML client encapsulates the configuration changes into an **ISexecCLI** request and sends it to the secondary backup router using HTTP. The server on the secondary backup side processes the incoming XML request and calls the Cisco IOS CLI parser to perform the updates.

For configuration information, see Configure Extension Assigner Synchronization.

Configure Extension Assigner

The following tasks are performed by an administrator or other personnel who is responsible for configuring Extension Assigner:

Determine Extension Numbers to Assign to the New Phones and Plan Your Configuration

After you determine which extension number to assign to each phone, you must make the following decisions:

- Which extension number must be dialed to access the extension assigner application.
- Whether the number is dialed automatically when a phone goes off hook.
- What password the installation technician must enter to access the extension assigner application.
- Whether to use ephone-tag (applicable only for SCCP phones) or the provision-tag number to identify the extension number to assign to the phone.
- How many temporary extension numbers to configure. This will determine how many temporary ephone-dns or voice register dns, and temporary MAC addresses to configure.
- What specific tag numbers to use to identify the extension number to assign to the phone.

Download the Tcl Script and Audio Prompt Files

To download the Tcl script and audio prompt files for the extension assigner feature, perform the following steps.

For more information about how to use Tcl scripts, see the Cisco IOS Tcl IVR and Voice XML Application Guide for your Cisco IOS release.

Note Do not edit the Tcl script

SUMMARY STEPS

1. Go to the Cisco Unified CME software download website at http://software.cisco.com/download/type.html?mdfid=277641082&catid=null.
2. Download the Cisco Unified CME extension assigner tar archive to a TFTP server that is accessible to the Cisco Unified CME router.
3. **enable**
4. **archive tar /xtract** *source-url destination-url*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Go to the Cisco Unified CME software download website at http://software.cisco.com/download/type.html?mdfid=277641082&catid=null.	Gives you access to Cisco Unified CME software downloads.

	Command or Action	Purpose
Step 2	Download the Cisco Unified CME extension assigner tar archive to a TFTP server that is accessible to the Cisco Unified CME router.	• This tar archive contains the extension assigner Tcl script and the default audio files that you need for the extension assigner service.
Step 3	**enable** **Example:** `Router> enable`	Enters global configuration mode.
Step 4	**archive tar /xtract** *source-url destination-url* **Example:** `Router# archive tar /xtract tftp://192.168.1.1/app-cme-ea-2.0.0.0.tar flash:`	Uncompresses the files in the archive file and copies them to a location that is accessible by the Cisco Unified CME router. • *source-url*—URL of the source of the extension assigner TAR file. Valid URLs can refer to TFTP or HTTP servers or to flash memory. • *location*—URL of the destination of the extension assigner TAR file, including its Tcl script and audio files. Valid URLs can refer to TFTP or HTTP servers or to flash memory.

Configure the Tcl Script

To configure and load the Tcl script for the extension assigner feature and create the password that installation technicians enter to access the extension assigner application, perform the following steps.

For more information about how to use Tcl scripts, see the Cisco IOS Tcl IVR and Voice XML Application Guide for your Cisco IOS release.

Note To change the password, you must remove the existing extension assigner service and create a new service that defines a new password.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **service** *service-name location*
5. **param ea-password** *password*
6. **paramspace english index** *number*
7. **paramspace english language** *en*
8. **paramspace english location** *location*
9. **paramspace english prefix en**
10. **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	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure packages and services.
Step 4	**service** *service-name location* **Example:** `Router(config-app)# service EA flash:/EA/`	Enters service parameter configuration mode to configure parameters for the call-queue service. • *service-name*—Name of the extension assigner service. This arbitrary name is used to identify the service during configuration tasks. • *location*—URL of the Tcl script for the extension assigner service. Valid URLs can refer to TFTP or HTTP servers or to flash memory.
Step 5	**param ea-password** *password* **Example:** `Router(config-app-param)# param ea-password 1234`	Sets the password that installation technicians enter to access the extension assigner application. • *password*—Numerical password that installation technicians enter to access the extension assigner application. Length: 2 to 10 digits.

	Command or Action	Purpose
Step 6	**paramspace english index** *number* **Example:** `Router(config-app-param)# paramspace english index 0`	Defines the language of audio files that are used for dynamic prompts by an IVR application. • For the Extension Assigner, language must be English and prefix is en.
Step 7	**paramspace english language** *en* **Example:** `Router(config-app-param)# paramspace english language en`	Defines the language of audio files that are used for dynamic prompts by an IVR application. • For the Extension Assigner, language must be English and prefix is en.
Step 8	**paramspace english location** *location* **Example:** `Router(config-app-param)# paramspace english location flash:/EA/`	Defines the location of audio files that are used for dynamic prompts by an IVR application. • For the Extension Assigner, language must be English. • *location*—URL of the Tcl script for the extension assigner service. Valid URLs can refer to TFTP or HTTP servers or to flash memory.
Step 9	**paramspace english prefix en** **Example:** `Router(config-app-param)# paramspace english prefix en`	Defines the prefix of audio files that are used for dynamic prompts by an IVR application. • For the Extension Assigner, language must be English and prefix is en.
Step 10	**end** **Example:** `Router(config-app-param)# end`	Returns to privileged EXEC mode.

Specify the Extension for Accessing Extension Assigner Application

To specify the extension number that installation technicians must dial to access the extension assigner application during onsite installation, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **service** *service-name* **out-bound**
5. **destination-pattern** *string*
6. **session protocol sipv2**
7. **session target ipv4:** *destination-address*
8. **dtmf-relay rtp-nte**
9. **codec** *g711ulaw*
10. **no vad**
11. **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* **voip** **Example:** `Router(config)# dial-peer voice 5999 voip`	Enters dial-peer configuration mode. • *tag*—Number used during configuration tasks to identify this dial peer.
Step 4	**service** *service-name* **out-bound** **Example:** `Router(config-dial-peer)# service extensionassigner out-bound`	Loads and configures the extension assigner application on a dial peer. • *service-name*—Name must match the name that you used to load the extension assigner Tcl script in the *Configuring the Tcl Script* section. • **outbound—**Required for Extension Assigner.
Step 5	**destination-pattern** *string* **Example:** `Router(config-dial-peer)# destination pattern 1010`	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) for a dial peer. • *string*—Number that the installation technician calls when assigning an extension number to a phone.

	Command or Action	Purpose
Step 6	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	Designates a SIP loopback trunk for Extension Assigner application.
Step 7	**session target ipv4:** *destination-address* **Example:** `Router(config-dial-peer)# session target ipv4:172.16.200.200`	Designates a network-specific address to receive calls from a VoIP dial peer. • *destination*-IP address for the Cisco Unified CME interface on this router.
Step 8	**dtmf-relay rtp-nte** **Example:** `Router(config-dial-peer)# dtmf-relay rtp-nte`	Specifies the method for relaying dual tone multifrequency (DTMF) tones between two devices as per RFC2833.
Step 9	**codec** *g711ulaw* **Example:** `Router(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for a dial peer. • *g711ulaw*-Option that represents the correct voice decoder rate. g711ulaw is the only codec supported with Extension Assigner application.
Step 10	**no vad** **Example:** `Router(config-dial-peer)# no vad`	Disables voice activity detection (VAD) for the calls using a particular dial peer. • Required for Extension Assigner.
Step 11	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Configure Provision-Tags for the Extension Assigner Feature

To modify Extension Assigner to use provision-tags, perform the following steps. By default, the extension assigner is enabled and uses ephone tags.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **extension-assigner tag-type** { **ephone-tag** | **provision-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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**extension-assigner tag-type** { **ephone-tag** | **provision-tag** } **Example:** `Router(config-telephony)# extension-assigner tag-type provision-tag`	Specifies tag type to use to identify extension numbers for Extension Assigner. • **ephone-tag** -Specifies that extension assigner use the ephone tag to identify the extension number that is assigned to a phone. The installation technician enters this number to assign an extension number to a phone. • **provision-tag**-Specifies that extension assigner use the provision-tag to identify the extension number that is assigned to a phone. The installation technician enters this number to assign an extension number to a phone.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Temporary Extension Numbers for SCCP Phones That Use Extension Assigner

To create ephone-dn that is used as temporary extension numbers for phones to which an extension number will be assigned by Extension Assigner, perform the following steps for each temporary number to be created.

Tip The readme file that is included with the script contains some sample entries for this procedure that you can edit to fit your needs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **trunk** *digit-string* [**timeout** *seconds*]
6. **name** *name*
7. **exit**
8. **telephony-service**
9. **auto assign** *dn-tag* **to** *dn-tag*
10. **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-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 90`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. **Note** We recommend that you use single-line mode for your temporary extension numbers.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 9000`	Configures a valid extension number for this ephone-dn instance.
Step 5	**trunk** *digit-string* [**timeout** *seconds*] **Example:** `Router(config-ephone-dn)# trunk 5999`	(Optional) Configures extension number to be automatically dialed for accessing the extension assigner application. • *digit-string* - Must match the number that you configured in the Specify the Extension for Accessing Extension Assigner Application section.
Step 6	**name** *name* **Example:** `RRouter(config-ephone-dn)# name hardware`	(Optional) Associates a name with this ephone-dn instance. This name is used for caller-ID displays and in the local directory listings. • Must follow the name order that is specified with the **directory** command.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 8	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 9	**auto assign** *dn-tag* **to** *dn-tag* **Example:** `Router(config-telephony)# auto assign 90 to 99`	Automatically assigns ephone-dn tags to Cisco Unified IP phones as they register for service with a Cisco Unified CME router. • Must match the tags that you configured in earlier step.
Step 10	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Temporary Extension Numbers for SIP Phones That Use Extension Assigner

To create voice register dns to use as temporary extension numbers for phones in which an extension number is assigned by Extension Assigner, perform the following steps for each temporary number to be created.

Tip The readme file that is included with the script contains some sample entries for this procedure that you can edit to fit your needs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **auto-register**
5. **password** *string*
6. **auto-assign** *first dn* **to** *last dn*
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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 4	**auto-register** **Example:** `Router(config-register-global)# auto-register`	Enters auto-register configuration mode.
Step 5	**password** *string* **Example:** `Router(config-voice-auto-register)# password xxxx`	Specifies default password for auto registered phones.
Step 6	**auto-assign** *first dn* **to** *last dn* **Example:** `Router(config-voice-auto-register)# auto-assign 90 to 99`	Automatically assigns voice register dn with these extensions to Cisco Unified IP phones as they register for service with a Cisco Unified CME router.
Step 7	**end** **Example:** `Router(config-voice-auto-register)# end`	Returns to privileged EXEC mode.

Configure Extension Numbers That Installation Technicians Can Assign to SCCP Phones

To create ephone-dns for an extension numbers that the installation technicians can assign to phones, perform the following steps for each directory number to be created.

Tip The readme file provided with this feature contains sample entries that you can edit to fit your needs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **trunk** *digit-string* [**timeout** *seconds*]
6. **name** name
7. **exit**
8. **telephony-service**
9. **auto assign** *dn-tag* **to** *dn-tag*
10. **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-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 20`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. **Note** To change an ephone-dn from dual-line to single-line mode or the reverse, first delete the ephone-dn and then recreate it.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 9000`	Configures a valid extension number for this ephone-dn instance.
Step 5	**trunk** *digit-string* [**timeout** *seconds*] **Example:** `Router(config-ephone-dn)# trunk 5999`	(Optional) Configures extension number to be automatically dialed for accessing the extension assigner application. • digit-string **-** Must match the number that you configured in the Specify the Extension for Accessing Extension Assigner Application section.
Step 6	**name** name **Example:** `Router(config-ephone-dn)# name hardware`	(Optional) Associates a name with this ephone-dn instance. This name is used for caller-ID displays and in the local directory listings.

	Command or Action	Purpose
		• Must follow the name order that is specified with the **directory** command.
Step 7	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode
Step 8	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 9	**auto assign** *dn-tag* **to** *dn-tag* **Example:** `Router(config-telephony)# auto assign 90 to 99`	Automatically assigns ephone-dn tags to Cisco Unified IP phones as they register for service with a Cisco Unified CME router. • Must match the tags that you configured in earlier step.
Step 10	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Extension Numbers That Installation Technicians Can Assign to SIP Phones

To create voice register dns for an extension numbers that the installation technicians can assign to phones, perform the following steps for each directory number to be created.

Tip The readme file provided with this feature contains sample entries that you can edit to fit your needs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *tag*
4. **number** *number*
5. **name** *name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register dn** *tag* **Example:** `Router(config)# voice register dn 20`	Enters voice register dn configuration mode, and creates a voice register dn.
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 20`	Configures a valid extension number for this voice register dn instance.
Step 5	**name** *name* **Example:** `Router(config-register-dn)# name hardware`	(Optional) Associates a name with this voice register dn instance. This name is used for caller-ID displays and in the local directory listings. • Must follow the name order that is specified with the **directory** command.
Step 6	**end** **Example:** `Router(config-register-dn)# end`	Returns to privileged EXEC mode.

Configure Ephones with Temporary MAC Addresses

Restriction To create an ephone configuration with temporary MAC address for a Cisco Unified CME phone to which you want the installation technician to assign extension numbers, perform the following steps for each phone.

- Max-ephone setting determines how many phones you can plug in at one time. For example, if your max-ephone setting is ten more than the number of phones to which you want to assign extension numbers, the you can plug in ten phones at a time. If you plug in eleven phones, one phone will not register or get a temporary extension number until you assign an extension to one of the first ten phones and reset the eleventh phone.
- For Cisco VG224 analog voice gateways with extension assigner, a minimum of 24 temporary ephones is required.

Tip The readme file provided with this feature contains some sample entries for this procedure that you can edit to fit your needs.

Before You Begin

The **max-ephone** command must be configured for a value equal to at least one greater than the number of phones to which you want to assign extension numbers to allow the autoregister feature to automatically create at least one ephone for your temporary extension numbers.

Note You are permitted to set the max-ephone value higher than the number of users supported by your Cisco Unified CME licenses for the purpose of enrolling licensed phones using Extension Assigner.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable** *phone-tag*
4. **provision-tag** *number*
5. **mac-address 02EA.EAEA.** *number*
6. **type** *phone-type* [**addon 1** *module-type* [*2 module-type*]]
7. **button** *button-number{separator}dn-tag*
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	**enable** *phone-tag* **Example:** `Router(config)# ephone 20`	Enters ephone configuration mode. • phone-tag-Maximum number is version and platform- specific. Type *?* to display range. • Number that the installation technician enters when assigning an extension to a phone if Extension Assigner uses ephone-tags (default).
Step 4	**provision-tag** *number* **Example:** `Router(config-ephone)# provision-tag 20`	(Optional) Creates a unique sequence number to be used by Extension Assigner to identify extension numbers to be assigned. • required only if you configured the **provision-tag** keyword with the **extension-assigner tag-type** command.
Step 5	**mac-address 02EA.EAEA.** *number* **Example:** `Router(config-ephone)# mac-address 02EA. EAEA. 0020`	Specifies a temporary MAC address number for this ephone. • For Extension Assigner, MAC address must begin with **02EA.EAEA.** • *number* - we strongly recommend that you make this number the same as the ephone number.
Step 6	**type** *phone-type* [**addon 1** *module-type* [*2 module-type*]] **Example:** `Router(config-ephone)# type 7960 addon 1 7914`	Specifies the type of phone.
Step 7	**button** *button-number{separator}dn-tag* **Example:** `Router(config-ephone)# button 1:1`	Associates a button number and line characteristics with an extension (ephone-dn). • Maximum number of buttons is determined by phone type. **Note** The Cisco Unified IP Phone 7910 has only one line button, but can be given two ephone-dn tags.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode

Configure Voice Register Pools with Temporary MAC Addresses

Restriction

- Max-pool setting determines how many phones you can plug in at one time. For example, if your max-pool setting is ten more than the number of phones to which you want to assign extension numbers, the you can plug in ten phones at a time. If you plug in eleven phones, one phone will not register or get a temporary extension number until you assign an extension to one of the first ten phones and reset the eleventh phone.

Tip The readme file provided with this feature contains some sample entries for this procedure that you can edit to fit your needs.

Before You Begin

The **max-pool** command must be configured for a value equal to at least one greater than the number of phones to which you want to assign extension numbers to allow the autoregister feature to automatically create at least one ephone for your temporary extension numbers.

Note

- You are permitted to set the max-pool value higher than the number of users supported by your Cisco Unified CME licenses for the purpose of enrolling licensed phones using Extension Assigner.
- For a phone that needs to invoke Extension Assigner application for assign or unassign operations, g711ulaw codec and dtmf-relay as rtp-nte needs to be configured in voice register pool.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **provision-tag** *number*
5. **mac-address 02EA.EAEA.** *number*
6. **type** *phone-type* [**addon 1** *module-type* [*2 module-type*]]
7. **number** *number* **dn** *dn-tag*
8. **dtmf-relay rtp-nte**
9. **codec** *g711ulaw*
10. **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 register pool** *pool-tag* **Example:** `Router(config)# voice register pool 20`	Enters voice register pool configuration mode. • phone-tag-Maximum number is version and platform- specific. Type *?* to display range. • Number that the installation technician enters when assigning an extension to a phone.
Step 4	**provision-tag** *number* **Example:** `Router(config-register-pool)# provision-tag 20`	Creates a unique sequence number to be used by Extension Assigner to identify extension numbers to be assigned. • required only if you configured the **provision-tag** keyword with the **extension-assigner tag-type** command.
Step 5	**mac-address 02EA.EAEA.** *number* **Example:** `Router(config-register-pool)# mac-address 02EA. EAEA. 0020`	Specifies a temporary MAC address number for this phone. • For Extension Assigner, MAC address must begin with **02EA.EAEA.** • *number* - we strongly recommend that you make this number same as the voice register pool number.

	Command or Action	Purpose
Step 6	**type** *phone-type* [**addon 1** *module-type* [*2 module-type*]] **Example:** `Router(config-register-pool)# type 8860 addon 1 CKEM 2`	Specifies the type of phone.
Step 7	**number** *number* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 1`	Associates number and line characteristics with an extension (voice register dn).
Step 8	**dtmf-relay rtp-nte** **Example:** `Router(config-register-pool)# dtmf-relay rtp-nte`	(Optional) Specifies the method for relaying dual tone multifrequency (DTMF) tones between two devices as per RFC2833. This configuration is required only to perform assign or unassign operation using Extension Assigner application.
Step 9	**codec** *g711ulaw* **Example:** `Router(config-register-pool)# codec g711ulaw`	(Optional) Specifies the voice coder rate of speech for a dial peer. This configuration is required only to perform assign or unassign operation using Extension Assigner application. • *g711ulaw*-Option that represents the correct voice decoder rate. g711ulaw is the only codec supported with Extension Assigner application.
Step 10	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Configure the Router to Automatically Save Your Configuration

To automatically save your router configuration when the router is restarted, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **kron policy-list** *list-name*
4. **cli write**
5. **exit**
6. **kron occurrence** *occurrence-name* [**user** *username*] [[**in** *numdays:*]*numhours:*]*nummin* { **oneshot** | **recurring** }
7. **policy-list** *list-name*
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	**kron policy-list** *list-name* **Example:** `Router(config)# kron policy-list save-config`	Specifies a name for a new or existing Command Scheduler policy list and enters kron-policy configuration mode. • If the value of the *list-name* argument is new, a new policy list structure is created. • If the value of the *list-name* argument exists, the existing policy list structure is accessed. No editor function is available, and the policy list is run in the order in which it was configured. **Note** You can also use the CLI command **background save interval** configured under telephony-service to automatically save configurations on Unified CME. This is as an alternative for the **kron** command.
Step 4	**cli write** **Example:** `Router(config-kron-policy)# cli write`	Specifies the fully-qualified EXEC command and associated syntax to be added as an entry in the Command Scheduler policy list.
Step 5	**exit** **Example:** `Router(config-kron-policy)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 6	**kron occurrence** *occurrence-name* [**user** *username*] [[**in** *numdays:*]*numhours:*]*nummin* { **oneshot** | **recurring** } **Example:** `Router(config)# kron occurrence backup in 30 recurring`	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode. • We recommend that you configure your router to save your configuration every 30 minutes. • *occurrence-name*-Specifies the name of the occurrence. Length of occurrence-name is from 1 to 31 characters. If the occurrence-name is new, an occurrence structure is created. If the occurrence-name is not new, the existing occurrence is edited. • **user**-(Optional) Used to identify a particular user. • *username*-Name of user. • **in**-Identifies that the occurrence is to run after a specified time interval. The timer starts when the occurrence is configured. • *numdays*:- (Optional) Number of days. If used, add a colon after the number. • *numhours*:- (Optional) Number of hours. If used, add a colon after the number. • *nummin*:- (Optional) Number of minutes. • **oneshot**-Identifies that the occurrence is to run only one time. After the occurrence has run, the configuration is removed. • **recurring**-Identifies that the occurrence is to run on a recurring basis.
Step 7	**policy-list** *list-name* **Example:** `Router(config-kron-occurrence)# policy-list save-config`	Specifies a Command Scheduler policy list.
Step 8	**end** **Example:** `Router(config-kron-occurrence)# end`	Returns to privileged EXEC mode.

Provide the Installation Technician with the Required Information

Before the installation technician can assign extension numbers to the new phones, you must provide the following information:

- How many phones the installation technician can plug in at one time. This is determined by the number of temporary MAC addresses that you configured.

- Which extension number to dial to access the extension assigner application.
- Whether the number is dialed automatically when a phone goes off hook (applicable only to SCCP phones).
- What password to enter to access the application.
- Which tag numbers to enter to assign an extension to each phone.

Configure Extension Assigner Synchronization

Configure the XML Interface for the Secondary Backup Router

To configure the secondary backup router to activate the XML interface required to receive configuration change information from the primary router, perform the following steps.

Note If there are HTTP connection issues between the primary router and the secondary backup router during automatic synchronization, the extension assigner synchronization changes are lost.

Restriction

- Automatic synchronization for new or replacement routers is not supported.
- Extension assigner preconfiguration must be manually performed on the secondary backup router.

Before You Begin

- The XML interface, provided through the Cisco IOS XML Infrastructure (IXI), must be configured. See Information About XML API.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service** | **voice register global**
4. **xml user** *user-name* **password** *password privilege-level*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**telephony-service | voice register global**
	
	Example:
	`Router(config)# telephony-service`
	`Router(config)# voice register global`
		Enters telephony service configuration mode or voice register global mode.

Step 4	**xml user** *user-name* **password** *password privilege-level*
	
	Example:
	`Router(config-telephony)# xml user user23 password 3Rs92uzQ 15`
	`Router(config-register-global)# xml user user23 password 3Rs92uzQ 15`
		Defines an authorized user.
		• *user-name*—Username of the authorized user.
		• *password*—Password to use for access.
		• *privilege-level*—Level of access to Cisco IOS commands to be granted to this user. Only the commands with the same or a lower level can be executed via XML. Range is 0 to 15.

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

Configure Extension Assigner Synchronization on the Primary Router

To configure the primary router to enable automatic synchronization to the secondary backup router, perform the following steps.

Before You Begin

- XML interface for secondary backup router is configured. See Configure the XML Interface for the Secondary Backup Router.
- The secondary backup router's IP address must already be configured using the **ip source-address** command in telephony-service configuration mode.

Note Phone configurations such as MAC address, pool-tag, and phone type are saved as part of synchronization for Extension Assigner feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service | voice register global**
4. **standby username** *username* **password** *password*
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	**telephony-service | voice register global**
	
	Example:
	`Router(config)# telephony-service`
	`Router(config)# voice register global`
		Enters telephony service configuration mode or voice register global mode.

Step 4	**standby username** *username* **password** *password*
	
	Example:
	`Router(config-telephony)# standby username user23 password 3Rs92uzQ`
	`Router(config-register-global)# standby username user23 password 3Rs92uzQ`
		Defines an authorized user.
		• Same username and password that was previously defined for the XML interface on the secondary backup router.

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

Assign Extension Numbers Onsite by Using Extension Assigner

The following tasks are performed by the installation technician at the customer's site:

Assign New Extension Numbers

Initially, when you install a phone, it is assigned a temporary, random extension number. To access Extension Assigner and assign the appropriate extension number to this phone, perform the following steps.

Step 1 Get the information you need to use extension assigner from your system administrator. For a list of this information, see Provide the Installation Technician with the Required Information.

Step 2 Dial the appropriate extension number to access the extension assigner system.

Step 3 Enter the password for the extension assigner and press #.

Step 4 Enter the ID number that represents this phone's extension and press #.

Step 5 If the extension is not assigned to another phone, press **1** to confirm that you want to assign the extension to your phone, then hang up. After the phone resets, the assignment is complete.

Step 6 If the extension is assigned to another phone that is idle:

a) Press **2** to confirm that you want to unassign the extension from the other phone.
b) Hang up.
c) Repeat this procedure beginning at Step 2, on page 378.

Step 7 If the extension is assigned to another phone that is in use, either:

- Return to Step 5, on page 378 to enter another extension number.
- Perform the procedures in the Unassign an Extension Number section and then repeat this procedure beginning at Step 2, on page 378.

Unassign an Extension Number

After the new extension number is assigned, you may find that you assigned the wrong number or that your original dial plan has changed. To unassign the wrong number so that it can be used by another phone, perform the following steps.

Note You can unassign the extension number of the phone that is used to dial in to the Extension Assigner or the extension number of another phone that has a provision-tag configured.

Step 1 Get the information you need to use extension assigner from your system administrator. For a list of this information, see Provide the Installation Technician with the Required Information.

Step 2 Dial the appropriate extension number to access the extension assigner system.

Step 3 Enter the password for the extension assigner and press #.

Step 4 Enter the provision-tag of the phone that needs to be unassigned, and press #.

Step 5 When you enter the provision-tag for the phone extension that needs to be unassigned, you are prompted to press **2** followed by # to confirm that you want to unassign the extension from the phone.

Step 6 Hang up.

Reassign the Current Extension Number

- If you must replace a broken phone or you want to reassign an extension number, perform the following steps.

Note You can reassign a number to a phone only if that number:

- Is not assigned to another phone
- Is assigned to another phone and that phone is idle
- Is assigned to another phone and you first unassign the extension

Step 1 Get the information you need to use extension assigner from your system administrator. For a list of this information, see Provide the Installation Technician with the Required Information.

Step 2 Dial the appropriate extension number to access the extension assigner system.

Step 3 Enter the password for the extension assigner and press #.

Step 4 Enter the ID number that represents this phone’s extension and press #.

Step 5 If the extension is not assigned to another phone, press **1** to confirm that you want to assign the extension to your phone, then hang up. After the phone resets, the reassignment is complete.

Step 6 If the extension is assigned to another phone that is idle:

- Press **2** to confirm that you want to unassign the extension from the other phone.
- Hang up.
- Perform the procedure in the Assign New Extension Numbers section.

Step 7 If the extension is assigned to another phone that is in use, either:

- Return to Step 5, on page 379 to enter another extension number.
- Perform the procedures in the Unassign an Extension Number section and the Assign New Extension Numbers section.

Verify Extension Assigner Configuration for SCCP Phones

Step 1 Use the **debug ephone extension-assigner** command to display status messages produced by the extension assigner application.

Step 2 Use the **debug voip application script** command to display status messages produced by the server as it runs the assigner application Tcl script.

Step 3 Use the **debug ephone state** command as described in the Cisco IOS Debug Command Reference.

Verify Extension Assigner Configuration for SIP Phones

Step 1 Use the **debug voice register events** and **debug voice register error** commands to display status messages produced by the extension assigner application.

Step 2 Use the **debug voip application script** command to display status messages produced by the server as it runs the assigner application Tcl script.

Step 3 Use the **debug ccsip messages** and **debug ccsip error** commands to display status messages for unregistration of phones.

Configuration Examples for Extension Assigner

Example for Extension Assigner on SCCP Phone

This example shows a router configuration with the following characteristics:

- The extension that the installation technician dials to access the extension assigner application is 0999.
- The password that the installation technician enters to access the extension assigner application is 1234.
- The **auto assign** command is configured to assign extensions 0001 to 0005.

- The installation technician can use extension assigner to assign extension numbers 6001 to 6005.
- The extension assigner uses the provision-tag to identify which ephone configuration and extension numbers to assign to the phone.
- The **auto-reg-ephone** command is shown but required, since it is enabled by default.
- The **kron** command is used to automatically save the router configuration.
- The max-ephone and max-dn settings of 51 are high enough to allow the installation technician to assign extensions to 50 phones, plugging them in one at a time. If the installation technician is assigning extensions to 40 phones, 11 can be plugged in one at a time. The exception is if you use Cisco VG224 Analog Voice Gateways. Extension assigner creates 24 ephones for each Cisco VG224 Analog Voice Gateway, one for each port.

```
Router# show running-config

version 12.4
no service password-encryption
!
hostname Test-Router
!
boot-start-marker
boot system flash:c2800nm-ipvoice-mz.2006-05-31.GOPED_DEV
boot-end-marker
!
enable password ww
!
no aaa new-model
!
resource policy
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool pool21
   network 172.21.0.0 255.255.0.0
   default-router 172.21.200.200

   option 150 ip 172.30.1.60
```

```
!
no ip domain lookup
!
application
 service EA flash:ea/app-cme-ea-2.0.0.0.tcl
  paramspace english index 0
  paramspace english language en
  param ea-password 1234
  paramspace english location flash:ea/
  paramspace english prefix en
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed 100
 no keepalive
!
interface GigabitEthernet0/0.21
 encapsulation dot1Q 21
 ip address 172.21.200.200 255.255.0.0
ip http server
!
control-plane
!
dial-peer voice 999 voip
 service EA out-bound
 destination-pattern 0999
 session target ipv4:172.21.200.200
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
!
telephony-service
 extension-assigner tag-type provision-tag
 max-ephones 51
 max-dn 51
 ip source-address 172.21.200.200 port 2000
 auto-reg-ephone
 auto assign 101 to 105
 system message Test-CME
 create cnf-files version-stamp 7960 Jun 14 2006 05:37:34
!
ephone-dn  1  dual-line
 number 6001
!
ephone-dn  2  dual-line
 number 6002
!
ephone-dn  3  dual-line
 number 6003
!
ephone-dn  4  dual-line
 number 6004
!
ephone-dn  5  dual-line
 number 6005
!
ephone-dn  101
 number 0101
 label Temp-Line-not assigned yet
!
ephone-dn  102
 number 0102
 label Temp-Line-not assigned yet
!
ephone-dn  103
 number 0103
 label Temp-Line-not assigned yet
!
ephone-dn  104
 number 0104
 label Temp-Line-not assigned yet
!
```

```
ephone-dn  105
 number 0105
 label Temp-Line-not assigned yet
!
ephone  1
 provision-tag 101
 mac-address 02EA.EAEA.0001
 button  1:1
!
ephone  2
 provision-tag 102
 mac-address 02EA.EAEA.0002
 button  1:2

!
ephone  3
 provision-tag 103
 mac-address 02EA.EAEA.0003
 button  1:3

!
ephone  4
 provision-tag 104
 mac-address 02EA.EAEA.0004
 button  1:4

!
ephone  5
 provision-tag 105
 mac-address 02EA.EAEA.0005
 button  1:5

!
kron occurrence backup in 30 recurring
policy-list writeconfig

!

kron policy-list writeconfig

cli write
!
line con 0
line aux 0
line vty 0 4
 logging synchronous
!
no scheduler max-task-time
scheduler allocate 20000 1000
!
end
```

Example for Extension Assigner on SIP Phone

The following example shows that provision tag 1001 is configured for voice register pool 1 and provision tag 1002 is configured for voice register pool 2:

```
voice register global
 auto-register
  password cisco1234
  auto assign 101-102

voice register dn 1001
 number 1001

voice register dn 1002
 number 1002

voice register pool 1
```

```
 provision-tag 1001
 mac-address 02EA.EAEA.0001
 number 1 dn 1001

voice register pool 2
 provision-tag 1002
 mac-address 02EA.EAEA.0002
 number 2 dn 1002
```

Example for Extension Assigner Synchronization

Primary Router: Example

The extension assigner is authorized to send configuration change information from the primary router to the secondary backup router.

```
telephony-service
standby username user555 password purplehat
```

Secondary Backup Router: Example

System components are enabled and the XML interface is readied to receive configuration change information.

```
ip http server
ixi transport http
     no shutdown
ixi application cme
     no shutdown
telephony-service
xml user user555 password purplehat 15
```

Feature Information for Extension Assigner

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

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

Table 20: Feature Information for Extension Assigner

Feature Name	Cisco Unfiied CME Version	Feature Information
Extension Assigner for SIP Phones	11.6	Enables the installation technicians to assign extension numbers to SIP Phones configured on Cisco Unified CME.
Extension Assigner Synchronization	4.2(1)	Enables the secondary backup router to automatically receive any changes made to ephone mac-addresess in the primary router.

Feature Name	Cisco Unfiied CME Version	Feature Information
Extension Assigner	4.0(3)	Enables installation technicians to assign extension numbers to Cisco Unified CME SCCP phones without accessing the server.

CHAPTER 9

Configuration Files for Phones

Information About Configuration Files

Configuration Files for Phones

When a phone requests service from Cisco Unified CME, the registrar confirms the username, i.e. the phone number for the phone. The phone accesses its configuration profile on the TFTP server, typically the Cisco Unified CME router, and processes the information contained in the file, registers itself, and puts the phone number on the phone console display.

Minimally, a configuration profile contains the MAC address, the type, and the phone number that is permitted by the registrar to handle the Register message for a particular Cisco Unified IP phone.

Any time you create or modify parameters for either an individual phone or a directory number, generate a new phone configuration to properly propagate the parameters.

By default, there is one shared XML configuration file located in system:/its/ for all Cisco Unified IP phones that are running SCCP. For SIP phones directly connected to Cisco Unified CME, an individual configuration profile is created for each phone and stored in system:/cme/sipphone/.

When an IP phone comes online or is rebooted, it automatically gets information about itself from the appropriate configuration file.

The Cisco universal application loader for phone firmware files allows you to add additional phone features across all protocols. To do this, a hunt algorithm searches for multiple configuration files. After a phone is reset or restarted, the phone automatically selects protocol depending on which *matching* configuration file is found first. To ensure that Cisco Unified IP phones download the appropriate configuration for the desired protocol, SCCP or SIP, you must properly configure the IP phones *before* connecting or rebooting the phones. The hunt algorithm searches for files in the following order:

1. CTLSEP <mac> file for a SCCP phone—For example, CTLSEP003094C25D2E.tlv

2 SEP <mac> file for a SCCP phone—For example, SEP003094C25D2E.cnf.xml

3 SIP <mac> file for a SIP phone—For example, SIP003094C25D2E.cnf or gk003069C25D2E

4 XML default file for SCCP phones—For example, SEPDefault.cnf.xmls

5 XML default file for SIP phones—For example, SIPDefault.cnf

In Cisco Unified CME 4.0 and later for SCCP and in Cisco CME 3.4 and later for SIP, you can designate one of the following locations in which to store configuration files:

- System (Default)—For SCCP phones, one configuration file is created, stored, and used for all phones in the system. For SIP phones, an individual configuration profile is created for each phone.
- Flash or slot 0—When flash or slot 0 memory on the router is the storage location, you can create additional configuration files to be applied per phone type or per individual phone, such as user or network locales.
- TFTP—When an external TFTP server is the storage location, you can create additional configuration files to be applied per phone type or per individual phone, which are required for multiple user and network locales.

Per-Phone Configuration Files

If configurations files for SCCP phones are to be stored somewhere other than in the default location, the following individual configuration files can be created for SCCP phones:

- Per phone type—Creates separate configuration files for each phone type and all phones of the same type use the same configuration file. This method is not supported if the configuration files are to be stored in the system location.
- Per phone—Creates a separate configuration file for each phone, by MAC address. This method is not supported if the configuration files are to be stored in the system location.

For configuration information, see Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.

Generate Configuration Files for Phones

Generate Configuration Files for SCCP Phones

To generate the configuration profile files that are required by the SCCP phones in Cisco Unified CME and write them to either system memory or to the location specified by the **cnf-file location** command, follow the steps in this section.

Restriction

- Externally stored and per-phone configuration files are not supported on the Cisco Unified IP Phone 7902G, 7910, 7910G, or 7920, or the Cisco Unified IP Conference Station 7935 and 7936.
- TFTP does not support file deletion. When configuration files are updated, they overwrite any existing configuration files with the same name. If you change the configuration file location, files are not deleted from the TFTP server.
- Generating configuration files on flash or slot 0 can take up to a minute, depending on the number of files being generated.
- F or smaller routers such as Cisco 2600 series routers, you must manually enter the **squeeze** command to erase files after changing the configuration file location or entering any commands that trigger the deletion of configuration files. Unless you use the **squeeze** command, the space used by the moved or deleted configuration files is not usable by other files.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **create cnf-files**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds the XML configuration files required for IP phones.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify Configuration Files for SCCP Phones

To verify the Cisco Unified CME phone configuration, perform the following steps.

Step 1 **show telephony-service all**
Use this command to verify the configuration for phones, directory numbers, voice ports, and dial peers in Cisco Unified CME.

Example:
`Router#` **show telephony-service all**

```
CONFIG (Version=4.0(0))
=====================
Version 4.0(0)
Cisco Unified CallManager Express
For on-line documentation please see:
www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html

ip source-address 10.0.0.1 port 2000
max-ephones 24
max-dn 24
dialplan-pattern 1 408734....
voicemail 11111
transfer-pattern 510734....
keepalive 30

ephone-dn 1
number 5001
huntstop

ephone-dn 2
number 5002
huntstop
call-forward noan 5001 timeout 8
```

Step 2 **show telephony-service tftp-bindings**
Use this command to display the current configuration files accessible to IP phones.

Example:
`Router#` **show telephony-service tftp-bindings**

```
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/XMLDefault7960.cnf.xml alias SEP00036B54BB15.cnf.xml
tftp-server system:/its/germany/7960-font.xml alias German_Germany/7960-font.xml
tftp-server system:/its/germany/7960-dictionary.xml alias German_Germany/7960-dictionary.xml
tftp-server system:/its/germany/7960-kate.xml alias German_Germany/7960-kate.xml
tftp-server system:/its/germany/SCCP-dictionary.xml alias German_Germany/SCCP-dictionary.xml
tftp-server system:/its/germany/7960-tones.xml alias Germany/7960-tones.xml
```

Generate Configuration Profiles for SIP Phones

To generate the configuration profile files that are required by the SIP phones in Cisco Unified CME and write them to the location specified by the **tftp-path (voice register global)** command, follow the steps in this section.

Any time you create or modify parameters under the voice register dn or voice register pool configuration modes, generate a new configuration profile and properly propagate the parameters.

Caution If your Cisco Unified CME system supports SCCP and also SIP phones, do not connect your SIP phones to the network until after you have verified the phone configuration profiles.

Before You Begin

- Cisco Unified CME 3.4 or a later version.
- The **mode** cme command must be enabled in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **file text**
5. **create profile**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**file text** **Example:** `Router(config-register-global)# file text`	(Optional) Generates ASCII text files of the configuration profiles generated for Cisco Unified IP Phone 7905s and 7905Gs, Cisco Unified IP Phone 7912s and 7912Gs, Cisco ATA-186, or Cisco ATA-188. • Default—System generates binary files to save disk space.
Step 5	**create profile** **Example:** `Router(config-register-global;)# create profile`	Generates configuration profile files required for SIP phones and writes the files to the location specified with **tftp-path** command.
Step 6	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

Verify Configuration Profiles for SIP Phones

To verify the configuration profiles, perform the following steps. SIP phones to be connected to Cisco Unified CME can register and minimally, have an assigned phone number, only if the configuration is correct.

Step 1 **show voice register tftp-bind**

Use this command to display a list of configuration profiles that are accessible to SIP phones using TFTP. The file name includes the MAC address for each SIP phone, such as SIP <mac-address>.cnf. Verify that a configuration profile is available for each SIP phone in Cisco Unified CME.

The following is sample output from this command:

Example:

`Router(config)#` **show voice register tftp-bind**

```
tftp-server SIPDefault.cnf url system:/cme/sipphone/SIPDefault.cnf>
tftp-server syncinfo.xml url system:/cme/sipphone/syncinfo.xml
tftp-server SIP0009B7F7532E.cnf url system:/cme/sipphone/SIP0009B7F7532E.cnf
tftp-server SIP000ED7DF7932.cnf url system:/cme/sipphone/SIP000ED7DF7932.cnf
tftp-server SIP0012D9EDE0AA.cnf url system:/cme/sipphone/SIP0012D9EDE0AA.cnf
tftp-server gk123456789012 url system:/cme/sipphone/gk123456789012
tftp-server gk123456789012.txt url system:/cme/sipphone/gk123456789012.txt
```

Step 2 **show voice register profile**

Use this command to display the contents of the ASCII format configuration profile for a particular voice register pool.

Note To generate ASCII text files of the configuration profiles for Cisco Unified IP Phone 7905s and 7905Gs, Cisco Unified IP Phone 7912s and 7912Gs, Cisco ATA-186s, and Cisco ATA-188s, use the **file text** command.

Example:

The following is sample output from this command displaying information in the configuration profile for voice register pool 4.

`Router#` **show voice register profile text 4**

```
Pool Tag: 4
# txt
AutoLookUp:0
DirectoriesUrl:0
…
CallWaiting:1
CallForwardNumber:0
Conference:1
AttendedTransfer:1
BlindTransfer:1
…
SIPRegOn:1
UseTftp:1
UseLoginID:0
UIPassword:0
NTPIP:0.0.0.0
UID:2468
```

Step 3 **more system**

Use this command to display the contents of the configuration profile for a particular Cisco Unified IP Phone 7940, Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7960, or Cisco Unified IP Phone 7960G.

The following is sample output from this command displaying information in two SIP configuration profile files. The SIPDefault.cnf configuration profile is a shared file and SIP < MAC address > .cnf is the SIP configuration profile for the SIP phone with the designated MAC address.

`Router#` **more system:/cme/sipphone/SIPDefault.cnf**

```
image_version: "P0S3-07-4-00";
proxy1_address: "10.1.18.100";
proxy2_address: "";
proxy3_address: "";
proxy4_address: "";
proxy5_address: "";
proxy6_address: "";
proxy1_port: "5060";
proxy2_port: "";
proxy3_port: "";
proxy4_port: "";
proxy5_port: "";
proxy6_port: "";
```

```
proxy_register: "1";
time_zone: "EST";
dst_auto_adjust: "1";
dst_start_month: "April";
dst_start_day: "";
dst_start_day_of_week: "Sun";
dst_start_week_of_month: "1";
dst_start_time: "02:00";
dst_stop_month: "October";
dst_stop_day: "";
dst_stop_day_of_week: "Sun";
dst_stop_week_of_month: "8";
dst_stop_time: "02:00";
date_format: "M/D/Y";
time_format_24hr: "0";
local_cfwd_enable: "1";
directory_url: "";
messages_uri: "2000";
services_url: "";
logo_url: "";
stutter_msg_waiting: "0";
sync: "0000200155330856";
telnet_level: "1";
autocomplete: "1";
call_stats: "0";
Domain_Name: "";
dtmf_avt_payload: "101";
dtmf_db_level: "3";
dtmf_inband: "1";
dtmf_outofband: "avt";
dyn_dns_addr_1: "";
dyn_dns_addr_2: "";
dyn_tftp_addr: "";
end_media_port: "32766";
http_proxy_addr: "";
http_proxy_port: "80";
nat_address: "";
nat_enable: "0";
nat_received_processing: "0";
network_media_type: "Auto";
network_port2_type: "Hub/Switch";
outbound_proxy: "";
outbound_proxy_port: "5060";
proxy_backup: "";
proxy_backup_port: "5060";
proxy_emergency: "";
proxy_emergency_port: "5060";
remote_party_id: "0";
sip_invite_retx: "6";
sip_retx: "10";
sntp_mode: "directedbroadcast";
sntp_server: "0.0.0.0";
start_media_port: "16384";
tftp_cfg_dir: "";
```

```
timer_invite_expires: "180";
timer_register_delta: "5";
timer_register_expires: "3600";
timer_t1: "500";
timer_t2: "4000";
tos_media: "5";
voip_control_port: "5060";
```

`Router#` **more system:/cme/sipphone/SIP000CCE62BCED.cnf**

```
image_version: "P0S3-07-4-00";
user_info: "phone";
line1_name: "1051";
line1_displayname: "";
line1_shortname: "";
line1_authname: "1051";
line1_password: "ww";
line2_name: "";
line2_displayname: "";
line2_shortname: "";
line2_authname: "";
line2_password: "";
auto_answer: "0";
speed_line1: "";
speed_label1: "";
speed_line2: "";
speed_label2: "";
speed_line3: "";
speed_label3: "";
speed_line4: "";
speed_label4: "";
speed_line5: "";
speed_label5: "";
call_hold_ringback: "0";
dnd_control: "0";
anonymous_call_block: "0";
callerid_blocking: "0";
enable_vad: "0";
semi_attended_transfer: "1";
call_waiting: "1";
cfwd_url: "";
cnf_join_enable: "1";
phone_label: "";
preferred_codec: "g711ulaw";
```

Where To Go Next

After you generate a configuration file for a Cisco Unified IP phone connected to the Cisco Unified CME router, you are ready to download the file to the phone. See Reset and Restart Phones, on page 399.

CHAPTER 10

Reset and Restart Cisco Unified IP Phones

Information About Resetting and Restarting Phones

Differences between Resetting and Restarting IP Phones

Cisco Unified IP phones must be rebooted after configuration changes in order for the changes to be effective. Configurations for phones in Cisco Unified CME are downloaded when a phone is rebooted or reset. You can reboot a single phone or you can reboot all phones in a Cisco Unified CME system. The differences between reboot types are summarized in Table 21: reset and restart Command Differences, on page 397.

> **Note** When rebooting multiple IP phones, it is possible for a conflict to occur if too many phones attempt to access changed Cisco Unified CME configuration information via TFTP simultaneously.

Table 21: reset and restart Command Differences

	reset Command	**restart Command**
Type of Reboot	Similar to power-off, power-on reboot.	Quick restart.
Phone Configurations	Downloads configurations for IP phones.	Downloads configurations for IP phones.

	reset Command	restart Command
DHCP and TFTP	Contacts DHCP and TFTP servers for updated configuration information. **Note** This command was introduced for SIP phones in Cisco CME 3.4.	Phones contact the TFTP server for updated configuration information and reregister without contacting the DHCP server. **Note** This command was introduced for SIP phones in Cisco Unified CME 4.1.
Processing Time	Takes longer to process when updating multiple phones.	Faster processing for multiple phones.
When Required	• Date and time settings • Network locale • Phone firmware • Source address • TFTP path • URL parameters • User locale • Voicemail access number Can be used when updating the following: • Directory numbers • Phone buttons • Speed-dial numbers	• Directory numbers • Phone buttons • Speed-dial numbers

Cisco Unified CME TAPI Enhancement

Before Cisco Unified CME 7.0(1), the only method to clear a session between a Microsoft Windows Workstation and an SCCP phone that was out-of-sync was to reboot the router. In Cisco Unified CME 7.0(1) and later versions, you can clear a Telephony Application Programming Interface (TAPI) session that is in a frozen state or out of synchronization by using a Cisco IOS software command. For configuration information, see Reset a Session Between a TAPI Application and an SCCP Phone, on page 401.

This enhancement also automatically handles ephone-TAPI registration error conditions. No additional configuration is required for this new feature.

Reset and Restart Phones

Note If phones are not yet plugged in, resetting or restarting phones is not necessary. Instead, connect your IP phones to your network to boot the phone and download the required configuration files.

Use the reset Command on SCCP Phones

To reboot and reregister one or more SCCP phones, including contacting the DHCP server for updated information, perform the following steps.

Before You Begin

- Phones to be rebooted are connected to the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service** or **ephone** *ephone-tag*
4. **reset** {**all** [*time-interval*] | **cancel** | **mac-address** *mac-address* | **sequence-all**} or **reset**
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	**telephony-service** or **ephone** *ephone-tag*
	
	Example:
	`Router(config)# telephony-service`
	or
	`Router(config)# ephone 1`
		Enters telephony-service configuration mode.
		or
		Enters ephone configuration mode.

	Command or Action	Purpose

Step 4	**reset** {**all** [*time-interval*] | **cancel** | **mac-address** *mac-address* | **sequence-all**} or **reset**
	
	Example:
	`Router(config-telephony)# reset all`
	or
	`Router(config-ephone)# reset`
		Performs a complete reboot of the specified or all phones running SCCP, including contacting the DHCP and TFTP servers for the latest configuration information.
		or
		Performs a complete reboot of the individual SCCP phone being configured.

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

Use the restart Command on SCCP Phones

To fast reboot and reregister one or more SCCP phones, perform the following steps.

Before You Begin

- Phones to be rebooted are connected to the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service** or **ephone** *ephone-tag*
4. **restart** {**all** [*time-interval*] | *mac-address*} or **restart**
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.

	Command or Action	Purpose

Step 3	**telephony-service** or **ephone** *ephone-tag*
	
	Example:
	`Router(config)# telephony-service`
	`or`
	`Router(config)# ephone 1`
		Enters telephony-service configuration mode.
		or
		Enters ephone configuration mode.

Step 4	**restart** {**all** [*time-interval*] | *mac-address*} or **restart**
	
	Example:
	`Router(config-telephony)# restart all`
	or
	`Router(config-ephone)# restart`
		Performs a fast reboot of the specified phone or all phones running SCCP associated with this Cisco Unified CME router. Does not contact the DHCP server for updated information.
		or
		Performs a fast reboot of the individual SCCP phone being configured.

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

Reset a Session Between a TAPI Application and an SCCP Phone

To clear a TAPI session that is in a frozen state or out of synchronization, perform the following steps.

Before You Begin

- Cisco Unified CME 7.0(1) or a later version

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **reset tapi**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 4	**reset tapi** **Example:** `Router(config-ephone)# reset tapi`	Resets the connection between a Telephony Application Programmer's Interface (TAPI) application and the SCCP phone.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Use the reset Command on SIP Phones

To reboot and reregister one or more SIP phones, including contacting the DHCP server for updated information, perform the following steps.

Before You Begin

- Cisco Unified CME 3.4 or later.
- The **mode** cme command must be enabled in Cisco Unified CME.
- Phones to be rebooted are connected to the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global** or **voice register pool** *pool-tag*
4. **reset**
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 register global** or **voice register pool** *pool-tag*
	
	Example:
	`Router(config)# voice register global`
	or
	`Router(config)# voice register pool 1`
		Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
		or
		Enters voice register pool configuration mode to set phone-specific parameters for SIP phones

Step 4	**reset**
	
	Example:
	`Router(config-register-global)# reset`
	or
	`Router(config-register-pool)# reset`
		Performs a complete reboot of all phones connected to this router that are running SIP, including contacting the DHCP and TFTP servers for the latest configuration information.
		or
		Performs a complete reboot of the individual SIP phone being configured.

Step 5	**end**
	
	Example:
	`Router(config-register-global)# end`
	or
	`Router(config-register-pool)# end`
		Exits to privileged EXEC mode.

Use the restart Command on SIP Phones

To fast reboot and reregister one or more SIP phones, perform the following steps.

Before You Begin

- Cisco Unified CME 4.1 or later.
- The **mode** cme command must be enabled in Cisco Unified CME.
- Phones to be rebooted are connected to the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global** or **voice register pool** *pool-tag*
4. **restart**
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 register global** or **voice register pool** *pool-tag*
	
	Example:
	`Router(config)# voice register global`
	or
	`Router(config)# voice register pool 1`
		Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
		or
		Enters voice register pool configuration mode to set phone-specific parameters for SIP phones.

Step 4	**restart**
	
	Example:
	`Router(config-register-global)# restart`
	or
	`Router(config-register-pool)# restart`
		Performs a fast reboot all SIP phones associated with this Cisco Unified CME router. Does not contact the DHCP server for updated information.
		or
		Performs a fast reboot of the individual SIP phone being configured.

Step 5	**end**
	
	Example:
	`Router(config-register-global)# end`
	or
	`Router(config-register-pool)# end`
		Exits configuration mode and enters privileged EXEC mode.

Verify Basic Call

To verify that Cisco IP phones in Cisco Unified CME can place and receive calls through the voice ports, perform the following steps.

Step 1 Test local phone operation. Make calls between phones on the Cisco Unified CME router.

Step 2 Place a call *from* a phone in Cisco Unified CME to a number in the local calling area.

Step 3 Place a call *to* a phone in Cisco Unified CME from a phone outside this Cisco Unified CME system.

Feature Information for Reset and Restart Phones

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

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

Table 22: Feature Information for Reset and Restart Phones

Feature Name	Cisco Unified CME Version	Feature Information
Cisco Unified CME TAPI Enhancement	7.0(1)	Disassociates and reestablishes a TAPI session that is in a frozen state or out of synchronization by using a Cisco IOS command. This enhancement also automatically handles ephone-TAPI registration error conditions.

CHAPTER 11

Localization Support

This chapter describes the localization support in Cisco Unified Communications Manager Express (Cisco Unified CME) for languages other than English and network tones and cadences not specific to the United States.

Information About Localization

Localization Enhancements in Cisco Unified CME

Cisco Unified CME supports the French locale but some phrases in France French and Canadian French differ. In Cisco Unified CME 9.5, Canadian French is supported as a user-defined locale on Cisco Unified SIP IP phones and Cisco Unified SCCP IP phones when the correct locale package is installed.

Note Some abbreviations such as BLF, SNR, and CME are not localized.

Prerequisites

- Cisco Unified CME 9.5 or later version
- Locale package version 9.5.2.6 is required

Restriction All the localization enhancements are supported in Cisco Unified CME only. They are not supported in Cisco Unified SRST. Table 23: Language Codes for User-Defined Locales, on page 408 shows the language codes used in the filenames of locale files.

Table 23: Language Codes for User-Defined Locales

Language	Language Code
Canadian French	fr_CA

For configuration information, see Install User-Defined Locales, on page 415.

System-Defined Locales

Cisco Unified CME provides built-in, system-defined localization support for 12 languages including English and 16 countries including the United States. Network locales specify country-specific tones and cadences; user locales specify the language to use for text displays.

Configuring system-defined locales depends on the type of IP phone:

- Cisco Unified IP Phone 7905, 7912, 7940, and 7960—System-defined network locales and user locales are preloaded into Cisco IOS software. No external files are required. Use the **network-locale** and **user-locale** commands to set the locales for these phones.
- Cisco Unified IP Phone 6921, 6945, 7906, 7911, 7921, 7931, 7941, 7961, 7970, 7971, 8941, 8945, and Cisco IP Communicator—You must download locale files to support the system-defined locales and store the files in flash memory, slot 0, or on an external TFTP server. See Install System-Defined Locales for Cisco Unified IP Phone 6921, 6945, 7906, 7911, 7921, 7931, 7941, 7961, 7970, 7971, and Cisco IP Communicator, on page 411.
- Cisco Unified 3905, 6941, 6945, 8961, 9951, and 9971 SIP IP Phones—You must download locale files to support the system-defined locales and store the files in flash memory, slot 0, or on an external TFTP server.

Note TFTP aliases for localization are not automatically created for Cisco Unified SIP IP phones in a Cisco Unified CME system. For more information on how to manually create TFTP aliases, see Install System-Defined Locales for Cisco Unified IP Phone 8961, 9951, and 9971, on page 427.

Note Cisco Unified CME 10.5 Release onwards, the System defined locales are deprecated and User-defined locales are recommended.

Cisco Unified 3905 SIP IP Phones and Cisco Unified 6945, 8941, and 8945 SCCP IP Phones have support for all locales up to Cisco Unified CME 8.8.

Localization Support for Cisco Unified SIP IP Phones

Cisco Unified CME 8.6 provides localization support for 12 languages including English and 16 countries including the United States. Network locales specify country-specific tones and cadences; user locales specify the language to use for text displays. Create additional localization support with user-defined locales. For more information about user-defined locales, see User-Defined Locales, on page 409.

In Cisco Unified CME 9.0 and later versions, localization is enhanced to support Cisco Unified 6941 and 6945 SIP IP Phones.

The **load** command supports both user-defined and system-defined locales.

Note The locale files must be stored in the same location as the configuration files.

User-Defined Locales

The user-defined locale feature allows you to support network and user locales other than the system-defined locales that are predefined in Cisco IOS software. For example, if your site has phones that must use the language and tones for Traditional Chinese, which is not one of the system-defined choices, you must install the locale files for Traditional Chinese.

In Cisco Unified CME 4.0 and later versions, you can download files to support a particular user and network locale and store the files in flash memory, slot 0, or an external TFTP server. These files cannot be stored in the system location. User-defined locales can be assigned to all phones or to individual phones.

User-defined language codes for user locales are based on ISO 639 codes, which are available at the Library of Congress website at http://www.loc.gov/standards/iso639-2/. User-defined country codes for network locales are based on ISO 3166 codes.

For configuration information, see Install User-Defined Locales, on page 415.

Localization Support for Phone Displays

On the Cisco Unified IP Phone 8961, 9951, and 9971, menus and prompts that are managed by the locale file for the IP phone type (.jar) or the Cisco Unified CME dictionary file are localized. Display options configured through Cisco IOS commands are not localized.

The following display items are localized by the IP phone (.jar file):

- System menus accessed with feature buttons (for example, messages, directories, services, settings, and information)
- Call processing messages
- Softkeys (for example, Redial and CFwdALL)

The following display items are localized by the dictionary file for Cisco Unified CME:

- Directory Service (Local Directory, Local Speed Dial, and Personal Speed Dial)
- Status Line

Display options configured through Cisco IOS commands are not localized and can only be displayed in English. For example, this includes features such as:

- Caller ID
- Header Bar
- Phone Labels
- System Message

Multiple Locales

In Cisco Unified CME 8.6 and later versions, you can specify up to five user and network locales and apply different locales to individual ephones or groups of ephones using ephone templates. For example, you can specify French for phones A, B, and C; German for phones D, E, and F; and English for phones G, H, and I. Only one user and network locale can be applied to each phone.

Each of the five user and network locales that you can define in a multilocale system is identified by a locale tag. The locale identified by tag 0 is always the default locale, although you can define this default to be any supported locale. For example, if you define user locale 0 to be JP (Japanese), the default user locale for all phones is JP. If you do not specify a locale for tag 0, the default is US (United States).

To apply alternative locales to different phones, you must use per-phone configuration files to build individual configuration files for each phone. The configuration files automatically use the default user-locale 0 and network-locale 0. You can override these defaults for individual phones by configuring alternative locale codes and then creating ephone-templates to assign the locales to individual ephones.

For configuration information, see Configure Multiple Locales on SCCP Phones, on page 422.

Locale Installer for Cisco Unified SCCP IP Phones

Before Cisco Unified CME 7.0(1), configuring localization required up to 16 steps, most of which were manual and some of which required filename changes. In Cisco Unified CME 7.0(1) and later versions, the following enhancements for installing locales are supported:

- Locale installer that supports a single procedure for all SCCP IP phones.
- Cisco Unified CME parses new firmware-load text files and automatically creates the TFTP aliases for localization, eliminating the requirement for you to manually create up to five aliases for files in the TAR file. To use this feature in Cisco Unified CME 7.0(1), you must use the complete filename, including the file suffix, when you configure the **load** command for phone firmware versions later than version 8-2-2 for all phone types. For example:

  `Router(config-telephony)#` **load 7941 SCCP41.8-3-3S.loads**

Note In Cisco Unified CME 4.3 and earlier versions, you do not include the file suffix for any phone type except Cisco ATA and Cisco Unified IP Phone 7905 and 7912. For example:

`Router(config-telephony)#` **load 7941 SCCP41.8-2-2SR2S**

- Backward compatibility with the configuration method in Cisco Unified CME 7.0 and earlier versions.

For configuration information, see Use the Locale Installer in Cisco Unified CME 7.0(1) and Later Versions, on page 419.

Locale Installer for Cisco Unified SIP IP Phones

Cisco Unified CME 9.0 and later versions support the following enhancements for installing locales for Cisco Unified SIP IP phones:

- Locale installer that supports a single procedure for all Cisco Unified SIP IP phones.
- New **load** keyword that requires you to use the complete filename, including the file suffix (.tar), when you configure the **user-locale** command for all Cisco Unified SIP IP phone types. The command syntax is **user-locale** [*user-locale-tag*] {[*user-defined-code*] *country-code*} [**load** *TAR-filename*]. For example,

  `Router(config-register-global)#`**user-locale 2 DE load CME-locale-de_DE-German-8.6.3.0.tar**

With the locale installer, you do not need to perform manual configuration. Instead, you copy the locale file using the **copy** command in privileged EXEC configuration mode.

Note

You must copy the locale file into the /its directory (flash:/its or slot0:/its) when you store the locale files on the Cisco Unified CME router.

For example,

`Router#` **copy tftp://12.1.1.100/CME-locale-de_DE-German-8.6.3.0.tar flash:/its**

For configuration information, see Use the Locale Installer in Cisco Unified CME 9.0 and Later Versions, on page 431.

Configure Localization Support on SCCP Phones

Install System-Defined Locales for Cisco Unified IP Phone 6921, 6945, 7906, 7911, 7921, 7931, 7941, 7961, 7970, 7971, and Cisco IP Communicator

Network locale files allow an IP phone to play the proper network tone for the specified country. You must download and install a tone file for the country you want to support.

User locale files allow an IP phone to display the menus and prompts in the specified language. You must download and install JAR files and dictionary files for each language you want to support.

To download and install locale files for system-defined locales, perform the following steps.

Tip

The locale installer simplifies the installation and configuration of system- and user-defined locales in Cisco Unified CME 7.0(1) and later versions. To use the locale installer in Cisco Unified CME 7.0(1) and later versions, see Use the Locale Installer in Cisco Unified CME 7.0(1) and Later Versions, on page 419.

Restriction

- Localization is not supported for SIP phones.
- Phone firmware, configuration files, and locale files must be in the same directory, except the directory file for Japanese and Russian, which must be in flash memory.

Before You Begin

- Cisco Unified CME 4.0(2) or a later version.
- You must create per-phone configuration files as described in Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- You must have an account on Cisco.com to download locale files.

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/CME-Locale.
You must have an account on Cisco.com to access the Software Download Center. If you do not have an account or if you have forgotten your username or password, click the appropriate button at the login dialog box and follow the instructions that appear.

Step 2 Navigate to **Downloads Home** > **Products** > **Unified Communications** > **Call Control** > **Mid-Market Call Control** > **Cisco Unified Communications Manager Express** > **Unified Communications Manager Express Individual File Set** and select your version of Cisco Unified CME.

Step 3 Select the TAR file for the locale you want to install. Each TAR file contains locale files for a specific language and country and uses the following naming convention: CME-locale-*language_country*-*CMEversion*

Example:
For example, CME-locale-de_DE-4.0.2-2.0 is German for Germany for Cisco Unified CME 4.0(2).

Step 4 Download the TAR file to a TFTP server that is accessible to the Cisco Unified CME router. Each file contains all the firmware required for all phone types supported by that version of Cisco Unified CME.

Step 5 Use the **archive tar** command to extract the files to flash memory, slot 0, or an external TFTP server.

Example:
`Router#` **archive tar /xtract** *source-url***flash:***/file-url*

Example:
For example, to extract the contents of CME-locale-de_DE-4.0.2-2.0.tar from TFTP server 192.168.1.1 to router flash memory, use this command:

`Router#` **archive tar /xtract tftp://192.168.1.1/cme-locale-de_DE-4.0.2-2.0.tar flash:**

Step 6 See Table 24: Phone-Type Codes for Locale JAR Files, on page 413 and Table 25: System-Defined User and Network Locales, on page 413 for a description of the codes used in the filenames and the list of supported directory names.
Each phone type has a JAR file that uses the following naming convention:

language-phone-sccp.jar

Example:

For example, de-td-sccp.jar is for German on the Cisco Unified IP Phone 7970.

Each TAR file also includes the file g3-tones.xml for country-specific network tones and cadences.

Table 24: Phone-Type Codes for Locale JAR Files

Phone Type	Phone Code
6921	rtl
6945	rtl
7906/7911	tc
7931	gp
7941/7961	mk
7970/7971	td
8941/8945	gh
CIPC	ipc

Table 25: System-Defined User and Network Locales

Language	Language Code	User-Locale Directory Name	Country Code	Network-Locale Directory Name
English	en	English_United_States[2]	US	United_States
		English_United_Kingdom	UK	United_Kingdom
			CA	Canada
Danish	dk	Danish_Denmark	DK	Denmark
Dutch	nl	Dutch_Netherlands	NL	Netherlands
French	fr	French_France	FR	France
			CA	Canada
German	de	German_Germany	DE	Germany
			AT	Austria
			CH	Switzerland

Language	Language Code	User-Locale Directory Name	Country Code	Network-Locale Directory Name
Italian	it	Italian_Italy	IT	Italy
Japanese[3]	jp	Japanese_Japan	JP	Japan
Norwegian	no	Norwegian_Norway	NO	Norway
Portuguese	pt	Portuguese_Portugal	PT	Portugal
Russian	ru	Russian_Russia	RU	Russian_Federation
Spanish	es	Spanish_Spain	ES	Spain
Swedish	se	Swedish_Sweden	SE	Sweden

2 English for the United States is the default language. You do not need to install the JAR file for U.S. English unless you assign a different language to a phone and then want to reassign English.

3 Katakana is supported by Cisco Unified IP Phone 7905, 7912, 7940, and 7960. Kanji is supported by Cisco Unified IP Phone 7911, 7941, 7961, 7970, and 7971.

Step 7 If you store the locale files in flash memory or slot 0 on the Cisco Unified CME router, create a TFTP alias for the user locale (text displays) and network locale (tones) using this format:

Example:

`Router(config)#` **tftp-server flash:/***jar_file***alias** *directory_name***/td-sccp.jar**
`Router(config)#` **tftp-server flash:/g3-tones.xml alias***directory_name***/g3-tones.xml**

Use the appropriate directory name shown in Table 25: System-Defined User and Network Locales, on page 413 and remove the two-letter language code from the JAR file name. For example, the TFTP aliases for German and Germany for the Cisco Unified IP Phone 7970 are:

`Router(config)#` **tftp-server flash:/de-td-sccp.jar alias German_Germany/td-sccp.jar**
`Router(config)#` **tftp-server flash:/g3-tones.xml alias Germany/g3-tones.xml**

Note On Cisco 3800 series routers, you must include /its in the directory name (flash:/its or slot0:/its). For example, the TFTP alias for German for the Cisco Unified IP Phone 7970 is: Router# **tftp-server flash:/its/de-td-sccp.jar alias German_Germany/td-sccp.jar**

Step 8 If you store the locale files on an external TFTP server, create a directory under the TFTP root directory for each user and network locale.
Use the appropriate directory name shown in Table 25: System-Defined User and Network Locales, on page 413 and remove the two-letter language code from the JAR file name.

Example:

For example, the user-locale directory for German and the network-locale directory for Germany for the Cisco Unified IP Phone 7970 are:

TFTP-Root/German_Germany/td-sccp.jar TFTP-Root/Germany/g3-tones.xml

Step 9 For Russian and Japanese, you must copy the UTF8 dictionary file into flash memory to use special phrases.

- Only flash memory can be used for these locales. Copy russian_tags_utf8_phrases for Russian; Japanese_tags_utf8_phrases for Japanese.
- Use the **user-locale jp** and **user-locale ru** command to load the UTF8 phrases into Cisco Unified CME.

Step 10 Assign the locales to phones. To set a default locale for all phones, use the **user-locale** and **network-locale** commands in telephony-service configuration mode.

Step 11 To support more than one user or network locale, see Configure Multiple Locales on SCCP Phones, on page 422.

Step 12 Use the **create cnf-files** command to rebuild the configuration files.

Step 13 Use the **reset** command to reset the phones and see the localized displays.

Install User-Defined Locales

You must download XML files for locales that are not predefined in the system. To install up to five user-defined locale files to use with phones, perform the following steps.

Note From Cisco Unified CME 10.5 Release onwards, the System defined locales are deprecated and User-defined locales are recommended. However, the older locale packages can be still used but some phrases may be displayed in English.

Restriction

- User-defined locales are not supported on the Cisco Unified IP Phone 7920 or 7936.
- User-defined locales are not supported if the configuration file location is “system:”.
- When you use the setup tool from the **telephony-service setup** command to provision phones, you can only choose a default user locale and network locale and you are limited to selecting a locale code that is supported in the system. You cannot use multiple locales or user-defined locales with the setup tool.
- When using a user-defined locale, the phone normally displays text using the user-defined fonts, except for any strings that are interpreted by Cisco Unified CME, such as “Cisco/Personal Directory,” “Speed Dial/Fast Dial,” and so forth.

Before You Begin

- Cisco Unified CME 4.0(3) or a later version.
- You must create per-phone configuration files as described in Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- You must have an account on Cisco.com to download locale files.

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/CME-Locale.

You must have an account on Cisco.com to access the Software Download Center. If you do not have an account or if you have forgotten your username or password, click the appropriate button at the login dialog box and follow the instructions that appear.

Step 2 Navigate to **Downloads Home** > **Products** > **Unified Communications** > **Call Control** > **Mid-Market Call Control** > **Cisco Unified Communications Manager Express** > **Unified Communications Manager Express Individual File Set** and select your version of Cisco Unified CME.

Step 3 Select the TAR file for the locale that you want to install. Each TAR file contains locale files for a specific language and country and uses the following naming convention: CME-locale-*language_country*-*CMEversion*-*fileversion*.

Example:
For example, CME-locale-zh_CN-4.0.3-2.0 is Traditional Chinese for China for Cisco Unified CME 4.0(3).

Step 4 Download the TAR file to a TFTP server that is accessible to the Cisco Unified CME router. Each file contains all the firmware required for all phone types supported by that version of Cisco Unified CME.

Step 5 Use the **archive tar** command to extract the files to slot 0, flash memory, or an external TFTP server.

Example:
`Router#` **archive tar /xtract** *source-url***flash:**/*file-url*

For example, to extract the contents of CME-locale-zh_CN-4.0.3-2.0.tar from TFTP server 192.168.1.1 to router flash memory, use this command:

`Router#` **archive tar /xtract tftp://192.168.1.1/cme-locale-zh_CN-4.0.3-2.0.tar flash:**

Step 6 For Cisco Unified IP Phone 7905, 7912, 7940, or 7960, go to Step 11, on page 418. For Cisco Unified IP Phone 7911, 7941, 7961, 7970, or 7971, go to Step 7, on page 416.

Step 7 Each phone type has a JAR file that uses the following naming convention: *language*-*type*-sccp.jar

Example:
For example, zh-td-sccp.jar is Traditional Chinese for the Cisco Unified IP Phone 7970.

See Table 26: Phone-Type Codes for Locale Files, on page 416 and Table 27: Language Codes for User-Defined Locales, on page 417 for a description of the codes used in the filenames.

Table 26: Phone-Type Codes for Locale Files

Phone Type	Code
6921	rtl
6945	rtl
7906/7911	tc
7931	gp
7941/7961	mk
7970/7971	td

Phone Type	Code
8941/8945	gh
CIPC	ipc

Table 27: Language Codes for User-Defined Locales

Language	Language Code
Bulgarian	bg
Chinese	zh[4]
Croation	hr
Czech Republic	cs
Finnish	fi
Greek	el
Hungarian	hu
Korean	ko
Polish	pl
Portugese (Brazil)	pt
Romanian	ro
Serbian	sr
Slovakian	sk
Slovenian	sl
Turkish	tr

4 For Cisco Unified IP Phone 7931, code for Chinese Simplified is chs; Chinese Traditional is cht.

Step 8 If you store the locale files in flash memory or slot 0 on the Cisco Unified CME router, create a TFTP alias using this format:

Example:

`Router(config)#` **tftp-server flash:**/*jar_file***alias** *directory_name*/**td-sccp.jar**

Remove the two-letter language code from the JAR filename and use one of five supported directory names with the following convention:

user_define_*number*, where *number* is 1 to 5

For example, the alias for Chinese on the Cisco Unified IP Phone 7970 is:

`Router(config)#` **tftp-server flash:/zh-td-sccp.jar alias user_define_1/td-sccp.jar**

Note On Cisco 3800 series routers, you must include /its in the directory name (flash:/its or slot0:/its). For example, the TFTP alias for Chinese for the Cisco Unified IP Phone 7970 is:

```
Router(config)# tftp-server flash:/its/zh-td-sccp.jar alias user_define_1/td-sccp.jar
```

Step 9 If you store the locale files on an external TFTP server, create a directory under the TFTP root directory for each locale. Remove the two-letter language code from the JAR filename and use one of five supported directory names with the following convention:

user_define_*number*, where *number* is 1 to 5

Example:

For example, for Chinese on the Cisco Unified IP Phone 7970, remove "zh" from the JAR filename and create the "user_define_1" directory under TFTP-Root on the TFTP server:

TFTP-Root/user_define_1/td-sccp.jar

Step 10 Go to Step 13, on page 419.

Step 11 Download one or more of the following XML files depending on your selected locale and phone type. All required files are included in the JAR file.

Example:

```
   7905-dictionary.xml
7905-font.xml
7905-kate.xml
7920-dictionary.xml
7960-dictionary.xml
7960-font.xml
7960-kate.xml
7960-tones.xml
SCCP-dictionary.utf-8.xml
SCCP-dictionary.xml
```

Step 12 Rename these files and copy them to flash memory, slot 0, or an external TFTP server. Rename the files using the format user_define_*number_filename* where *number* is 1 to 5.

Example:

For example, use the following names if you are setting up the first user-locale:

```
   user_define_1_7905-dictionary.xml
user_define_1_7905-font.xml
user_define_1_7905-kate.xml
user_define_1_7920-dictionary.xml
user_define_1_7960-dictionary.xml
user_define_1_7960-font.xml
user_define_1_7960-kate.xml
user_define_1_7960-tones.xml
```

```
user_define_1_SCCP-dictionary.utf-8.xml
user_define_1_SCCP-dictionary.xml
```

Step 13 Copy the *language*_tags_file and *language*_utf8_tags_file to the location of the other locale files (flash memory, slot 0, or TFTP server). Rename the files to user_define_*number*_tags_file and user_define_*number*_utf8_tags_file respectively, where*number* is 1 to 5 and matches the user-defined directory.

Step 14 Assign the locales to phones. See Configure Multiple Locales on SCCP Phones, on page 422.

Step 15 Use the **create cnf-files** command to rebuild the configuration files.

Step 16 Use the **reset** command to reset the phones and see the localized displays.

Use the Locale Installer in Cisco Unified CME 7.0(1) and Later Versions

To install and configure locale files to use with SCCP phones in Cisco Unified CME, perform the following steps.

Tip Cisco Unified CME 7.0(1) provides backward compatibility with the configuration method in Cisco Unified CME 4.3/7.0 and earlier versions. To use the same procedures as you used with earlier versions of Cisco Unified CME, see Install System-Defined Locales for Cisco Unified IP Phone 6921, 6945, 7906, 7911, 7921, 7931, 7941, 7961, 7970, 7971, and Cisco IP Communicator, on page 411.

Restriction

- When using an external TFTP server, you must manually create the user locale folders in the root directory. This is a limitation of the TFTP server.
- Locale support is limited to phone firmware versions that are supported by Cisco Unified CME.
- User-defined locales are not supported on the Cisco Unified IP Phone 7920 or 7936.
- User-defined locales are not supported if the configuration file location is system.
- When you use the setup tool from the **telephony-service setup** command to provision phones, you can only choose a default user locale and network locale, and you are limited to selecting a locale code that is supported in the system. You cannot use multiple locales or user-defined locales with the setup tool.
- When using a user-defined locale, the phone normally displays text using the user-defined fonts, except for any strings that are interpreted by Cisco Unified CME, such as "Cisco/Personal Directory," and "Speed Dial/Fast Dial."
- If you install and configure a user-defined locale using country codes U1-U5 and then you install a new locale using the same label, the phone retains the original language locale even after the phone is reset. This is a limitation of the IP phone. To work around this limitation, you must configure the new package using a different country code.
- Each user-defined country code (U1-U5) can be used for only one user-locale-tag at a time. For example:

```
Router(config-telephony)# user-locale 2 U2 load Finnish.pkg
Router(config-telephony)# user-locale 1 U2 load Chinese.pkg
LOCALE ERROR: User Defined Locale U2 already exists on locale index 2.
```

Before You Begin

- Cisco Unified CME 7.0(1) or a later version.
- You must configure Cisco Unified CME for per-phone configuration files. See Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- When the storage location specified by the **cnf-file location** command is flash memory, sufficient space must be on the flash file system for extracting the contents of the locale TAR file.
- You must have an account on Cisco.com to download locale files.

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/CME-Locale.
You must have an account on Cisco.com to access the Software Download Center. If you do not have an account or have forgotten your username or password, click the appropriate button at the login dialog box and follow the instructions that appear.

Step 2 Navigate to **Downloads Home** > **Products** > **Unified Communications** > **Call Control** > **Mid-Market Call Control** > **Cisco Unified Communications Manager Express** > **Unified Communications Manager Express Individual File Set** and select your version of Cisco Unified CME.

Step 3 Select the TAR file for the locale you want to install. Each TAR file contains locale files for a specific language and country and uses the following naming convention: CME-locale-*language_country-CMEversion*

Example:
For example, CME-locale-de_DE-7.0.1.0 is German for Germany for Cisco Unified CME 7.0(1).

Step 4 Download the TAR file to the location previously specified by the **cnf-file location** command. Each file contains all the firmware required for all phone types supported by that version of Cisco Unified CME.

a) If the cnf-file location is flash memory: Copy the TAR file to the flash:/its directory.
b) If the cnf-file location is slot0: Copy the TAR file to the slot0:/its directory.
c) If the cnf-file location is tftp: Create a folder in the root directory of the TFTP server for each locale using the following format and then copy the TAR file to the TFTP-Root folder. **TFTP-Root**/*TAR-filename*

Example:
For system-defined locales, use the locale folder name as shown in Table 28: System-Defined and User-Defined Locales, on page 421. For example, create the folder for system-defined German as follows:

TFTP-Root/de_DE-7.0.1.0.tar

For up to five user-defined locales, use the User_Define_*n* folder name as shown in Table 28: System-Defined and User-Defined Locales, on page 421. A user-defined locale is a language other than the system-defined locales that are predefined in Cisco IOS software. For example, create the folder for user-defined locale Chinese (User_Define_1) as follows:

TFTP-Root/CME-locale-zh_CN-7.0.1.0.tar

Note For a list of user-defined languages supported in Cisco Unified CME, see Cisco Unified CME Localization Matrix.

Table 28: System-Defined and User-Defined Locales

Language	Locale Folder Name	Country Code
English	English_United_States	US
	English_United_Kingdom	UK
		CA
Danish	Danish_Denmark	DK
Dutch	Dutch_Netherlands	NL
French	French_France	FR
		CA
German	German_Germany	DE
		AT
		CH
Italian	Italian_Italy	IT

Language	Locale Folder Name	Country Code
Japanese[5]	Japanese_Japan	JP
Norwegian	Norwegian_Norway	NO
Portuguese	Portuguese_Portugal	PT
Russian	Russian_Russia	RU
Spanish	Spanish_Spain	ES
Swedish	Swedish_Sweden	SE
Un[6]	User_Define_n[2]	Un[2]

5 Katakana is supported by Cisco Unified IP Phone 7905, 7912, 7940, and 7960. Kanji is supported by Cisco Unified IP Phone 7911, 7941, 7961, 7970, and 7971.

6 Where "n" is a number from 1 to 5.

Step 5 Use the **user-locale** [*user-locale-tag*] *country-code***load** *TAR-filename* command in telephony-service configuration mode to extract the contents of the TAR file. For country codes, see Table 28: System-Defined and User-Defined Locales, on page 421.

Example:

For example, to extract the contents of the CME-locale-zh_CN-7.0.1.0.tar file when U1 is the country code for user-defined locale Chinese (User_Define_1), use this command:

```
Router (telephony-service)# user-locale U1 load CME-locale-zh_CN-7.0.1.0.tar
```

Step 6 Assign the locales to phones. See Configure Multiple Locales on SCCP Phones, on page 422.

Step 7 Use the **create cnf-files** command to rebuild the configuration files.

Step 8 Use the **reset** command to reset the phones and see the localized displays.

Verify User-Defined Locales

See Verify Multiple Locales on SCCP Phones, on page 426.

Configure Multiple Locales on SCCP Phones

To define one or more alternatives to the default user and network locales and apply them to individual phones, perform the following steps.

Restriction

- Multiple user and network locales are not supported on the Cisco Unified IP Phone 7902G, 7910, 7910G, or 7920, or the Cisco Unified IP Conference Stations 7935 and 7936.
- When you use the setup tool from the **telephony-service setup** command to provision phones, you can only choose a default user locale and network locale and you must select a locale code that is predefined in the system. You cannot use multiple or user-defined locales with the setup tool.

Before You Begin

- Cisco Unified CME 4.0 or a later version.
- To specify alternative user and network locales for individual phones in a Cisco Unified CME system, you must use per-phone configuration files. For more information, see Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- You can also use user-defined locale codes as alternative locales after you download the appropriate XML files. See Install User-Defined Locales, on page 415.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **user-locale** [*user-locale-tag*] {[*user-defined-code*] *country-code*}
5. **network-locale** *network-locale-tag* [*user-defined-code*] *country-code*
6. **create cnf-files**
7. **exit**
8. **ephone-template** *template-tag*
9. **user-locale** *user-locale-tag*
10. **network-locale** *network-locale-tag*
11. **exit**
12. **ephone** *phone-tag*
13. **ephone-template** *template-tag*
14. **exit**
15. **telephony-service**
16. **reset** {**all** [*time-interval*]| **cancel** | **mac-address** *mac-address* | **sequence-all**}
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**user-locale** [*user-locale-tag*] {[*user-defined-code*] *country-code*} **Example:** `Router(config-telephony)# user-locale 1 U1 ZH`	Specifies a language for phone displays. • *user-locale-tag*—Assigns a locale identifier to the locale. Range is 0 to 4. Default: 0. This argument is required when defining some locale other than the default (0). • *user-defined-code*—(Optional) Assigns one of the user-defined codes to the specified country code. Valid codes are **U1**, **U2**,**U3**, **U4**, and **U5**. • *country-code*—Type **?** to display a list of system-defined codes. Default: US (United States). You can assign any valid ISO 639 code to a user-defined code (U1 to U5).
Step 5	**network-locale** *network-locale-tag* [*user-defined-code*] *country-code* **Example:** `Router(config-telephony)# network-locale 1 FR`	Specifies a country for tones and cadences. • *network-locale-tag*—Assigns a locale identifier to the country code. Range is 0 to 4. Default: 0. This argument is required when defining some locale other than the default (0). • *user-defined-code*—(Optional) Assigns one of the user-defined codes to the specified country code. Valid codes are **U1**, **U2**,**U3**, **U4**, and **U5**. • *country-code*—Type **?** to display a list of system-defined codes. Default: US (United States). You can assign any valid ISO 3166 code to a user-defined code (U1 to U5).
Step 6	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds the required XML configuration files for IP phones. Use this command after you update configuration file parameters such as the user locale or network locale.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 8	**ephone-template** *template-tag* **Example:** `Router(config)# ephone template 1`	Enters ephone-template configuration mode. • *template-tag*—Unique sequence number that identifies this template during configuration tasks.
Step 9	**user-locale** *user-locale-tag* **Example:** `Router(config-ephone-template)# user-locale 2`	Assigns a user locale to this ephone template. • *user-locale-tag*—A locale tag that was created in Step 4, on page 424. Range is 0 to 4.
Step 10	**network-locale** *network-locale-tag* **Example:** `Router(config-ephone-template)# network-locale 2`	Assigns a network locale to this ephone template. • *network-locale-tag*—A locale tag that was created in Step 5, on page 424. Range is 0 to 4.
Step 11	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 12	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 13	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 1`	Applies an ephone template to an ephone. • *template-tag*—Number of the template to apply to this ephone.
Step 14	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode.
Step 15	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 16	**reset** {**all** [*time-interval*]| **cancel** | **mac-address** *mac-address* | **sequence-all**} **Example:** `Router(config-telephony)# reset all`	Performs a complete reboot of all phones or the specified phone, including contacting the DHCP and TFTP servers for the latest configuration information. • **all—**All phones in the Cisco Unified CME system. • *time-interval***—**(Optional) Time interval, in seconds, between each phone reset. Range is 0 to 60. Default is 15. • *cancel***—**Interrupts a sequential reset cycle that was started with a **reset sequence-all** command. • **mac-address** *mac-address***—**A specific phone. • **sequence-all—**Resets all phones in strict one-at-a-time order by waiting for one phone to reregister before starting the reset for the next phone.
Step 17	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify Multiple Locales on SCCP Phones

Step 1 Use the **show telephony-service tftp-bindings** command to display a list of configuration files that are accessible to IP phones using TFTP, including the dictionary, language, and tone configuration files.

Example:

```
Router(config)# show telephony-service tftp-bindings

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/XMLDefault7960.cnf.xml alias SEP00036B54BB15.cnf.xml
tftp-server system:/its/germany/7960-font.xml alias German_Germany/7960-font.xml
tftp-server system:/its/germany/7960-dictionary.xml alias German_Germany/7960-dictionary.xml
tftp-server system:/its/germany/7960-kate.xml alias German_Germany/7960-kate.xml
tftp-server system:/its/germany/SCCP-dictionary.xml alias German_Germany/SCCP-dictionary.xml
tftp-server system:/its/germany/7960-tones.xml alias Germany/7960-tones.xml
```

Step 2 Ensure that per-phone configuration files are defined with the **cnf-file perphone** command.

Step 3 Use the **show telephony-service ephone-template** command to check the user locale and network locale settings in each ephone template.

Step 4 Use the **show telephony-service ephone** command to check that the correct templates are applied to phones.

Step 5 If the configuration file location is not TFTP, use the **debug tftp events** command to see which files Cisco Unified CME is looking for and whether the files are found and opened correctly. There are usually three states ("looking for x file," "opened x file," and "finished x file"). The file is found when all three states are displayed. For an external TFTP server you can use the logs from the TFTP server.

Configure Localization Support on SIP Phones

Install System-Defined Locales for Cisco Unified IP Phone 8961, 9951, and 9971

Network locale files allow an IP phone to play the proper network tone for the specified country. You must download and install a tone file for the country you want to support.

User locale files allow an IP phone to display the menus and prompts in the specified language. You must download and install JAR files and dictionary files for each language you want to support.

To download and install locale files for system-defined locales, perform the following steps.

Restriction Phone firmware, configuration files, and locale files must be in the same directory.

Before You Begin

- Cisco Unified CME 8.6 or a later version. For Cisco Unified IP Phone 9971, Cisco Unified CME 8.8 or a later version.
- You must have an account on Cisco.com to download locale files.

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/CME-Locale.
You must have an account on Cisco.com to access the Software Download Center. If you do not have an account or if you have forgotten your username or password, click the appropriate button at the login dialog box and follow the instructions that appear.

Step 2 Navigate to **Downloads Home** > **Products** > **Unified Communications** > **Call Control** > **Mid-Market Call Control** > **Cisco Unified Communications Manager Express** > **Unified Communications Manager Express Individual File Set** and select your version of Cisco Unified CME.

Step 3 Select the TAR file for the locale you want to install. Each TAR file contains locale files for a specific language and country and uses the following naming convention: CME-locale-*language_country-CMEversion*

Example:

For example, CME-locale-de_DE-8.6 is German for Germany for Cisco Unified CME 8.6.

Step 4 Download the TAR file to a TFTP server that is accessible to the Cisco Unified CME router. Each file contains all the firmware required for all phone types supported by that version of Cisco Unified CME.

Step 5 Use the **archive tar** command to extract the files to flash memory, slot 0, or an external TFTP server.

Example:

`Router#` **archive tar /xtract** *source-url***flash:***/file-url*

For example, to extract the contents of CME-locale-de_DE-8.6.tar from TFTP server 192.168.1.1 to router flash memory, use this command:

`Router#` **archive tar /xtract tftp://192.168.1.1/cme-locale-de_DE-8.6.tar flash:**

Step 6 See Table 29: Phone-Type Codes for Locale JAR Files, on page 428 and Table 30: System-Defined User and Network Locales , on page 429 for a description of the codes used in the filenames and the list of supported directory names. Each phone type has a JAR file that uses the following naming convention:

language-phone-sip.jar

Example:

For example, de-gh-sip.jar is for German on the Cisco Unified IP Phone 8961.

Each TAR file also includes the file g4-tones.xml for country-specific network tones and cadences.

Table 29: Phone-Type Codes for Locale JAR Files

Phone Type	Phone Code
3905	cin
6941	rtl
6945	rtl
8961	gh
9951	gd
9971	gd

Table 30: System-Defined User and Network Locales

Language	Language Code	User-Locale Directory Name	Country Code	Network-Locale Directory Name
English	en	English_United_States[7]	US	United_States
		English_United_Kingdom	UK	United_Kingdom
			GB	United_Kingdom
			CA	Canada
			AU	Australia
Danish	dk	Danish_Denmark	DK	Denmark
Dutch	nl	Dutch_Netherlands	NL	Netherlands
French	fr	French_France	FR	France
			CA	Canada
German	de	German_Germany	DE	Germany
			AT	Austria
			CH	Switzerland
Italian	it	Italian_Italy	IT	Italy
Japanese	jp	Japanese_Japan	JP	Japan
Norwegian	no	Norwegian_Norway	NO	Norway
Portuguese	pt	Portuguese_Portugal	PT	Portugal
Russian	ru	Russian_Russia	RU	Russian_Federation
Spanish	es	Spanish_Spain	ES	Spain
Swedish	se	Swedish_Sweden	SE	Sweden

7 English for the United States is the default language. You do not need to install the JAR file for U.S. English unless you assign a different language to a phone and then want to reassign English.

Step 7 If you store the locale files in flash memory or slot 0 on the Cisco Unified CME router, create a TFTP alias for the user locale (text displays) and network locale (tones) using this format:

Example:

Router(config)# **tftp-server flash:/***jar_file***alias** *directory_name*/**gh-sip.jar**
Router(config)# **tftp-server flash:/g4-tones.xml alias***directory_name*/**g4-tones.xml**

Use the appropriate directory name shown in Table 29: Phone-Type Codes for Locale JAR Files, on page 428 and remove the two-letter language code from the JAR file name.

For example, the TFTP aliases for German and Germany for the Cisco Unified IP Phone 8961 are:

Router(config)# **tftp-server flash:/de-gh-sip.jar alias German_Germany/**
Router(config)# **tftp-server flash:/g4-tones.xml alias Germany/g4-tones.xml**

Step 8 If you store the locale files on an external TFTP server, create a directory under the TFTP root directory for each user and network locale.
Use the appropriate directory name shown in Table 29: Phone-Type Codes for Locale JAR Files, on page 428 and remove the two-letter language code from the JAR file name.

Example:

For example, the user-locale directory for German and the network-locale directory for Germany for the Cisco Unified IP Phone 8961 are:

TFTP-Root/German_Germany/gh-sip.jar TFTP-Root/Germany/g4-tones.xml

Step 9 Assign the locales to the phones. To set a default locale for all phones, use the **user-locale** and **network-locale** commands in voice register global configuration mode.

Step 10 To support more than one user or network locale, see Verify Multiple Locales on SIP Phones, on page 437.

Step 11 Use the **create profile** command to rebuild the configuration files.

Step 12 Use the **reset** command to reset the phones and see the localized displays.

Use the Locale Installer in Cisco Unified CME 9.0 and Later Versions

Restriction

- When using an external TFTP server, you must manually create the user locale folders in the root directory. This is a limitation of the TFTP server.
- Locale support is limited to phone firmware versions that are supported by Cisco Unified CME.
- User-defined locales are not supported if the configuration file location is "system:".
- If you install and configure a user-defined locale using country codes U1-U5 and then you install a new locale using the same label, the phone retains the original language locale even after the phone is reset. This is a limitation of the IP phone. To work around this limitation, you must configure the new package using a different country code.
- Each user-defined country code (U1-U5) can be used for only one user-locale-tag at a time. For example:

```
Router(config-register-global)# user-locale 2 U2 load Finnish.pkg
Router(config-register-global)# user-locale 1 U2 load Chinese.pkg
LOCALE ERROR: User Defined Locale U2 already exists on locale index 2.
```

Before You Begin

- Cisco Unified CME 9.0(1) or a later version.
- When the storage location specified by the **cnf-file location** command is flash memory, sufficient space must be on the flash file system for extracting the contents of the locale TAR file.
- You must have an account on Cisco.com to download locale files.

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/CME-Locale
You must have an account on Cisco.com to access the Software Download Center. If you do not have an account or have forgotten your username or password, click the appropriate button at the login dialog box and follow the instructions that appear.

Step 2 Navigate to **Downloads Home** > **Products** > **Unified Communications** > **Call Control** > **Mid-Market Call Control** > **Cisco Unified Communications Manager Express** > **Unified Communications Manager Express Individual File Set** and select your version of Cisco Unified CME.

Step 3 Select the TAR file for the locale you want to install. Each TAR file contains locale files for a specific language and country and uses the following naming convention: CME-locale-*language_country-CMEversion*.tar

Example:
For example, CME-locale-de_DE-German-8.6.3.0.tar is German for Germany for Cisco Unified CME 9.0.

Step 4 Download the TAR file to the location previously specified by the **cnf-file location** command. Each file contains all the firmware required for all phone types supported by that version of Cisco Unified CME.
With the locale installer, you do not need to perform manual configuration. Instead, you copy the locale file using the **copy** command in privileged EXEC configuration mode.

Note You must copy the locale file into the /its directory (flash:/its or slot0:/its) when you store the locale files on the Cisco Unified CME router.

a) If the cnf-file location is flash memory: Copy the TAR file to the flash:/its directory.

Example:
For example,

`Router#` **copy tftp://12.1.1.100/CME-locale-de_DE-German-8.6.3.0.tar flash:/its**

b) If the cnf-file location is slot0: Copy the TAR file to the slot0:/its directory.

c) If the cnf-file location is tftp: Create a folder in the root directory of the TFTP server for each locale using the following format and then copy the TAR file to the TFTP-Root folder.

Example:
TFTP-Root/*TAR-filename*

For system-defined locales, use the locale folder name as shown in Table 31: System-Defined and User-Defined Locales , on page 432. For example, create the folder for system-defined German as follows:

TFTP-Root/de_DE-8.6.3.0.tar

For up to five user-defined locales, use the User_Define_*n* folder name as shown in Table 31: System-Defined and User-Defined Locales , on page 432. A user-defined locale is a language other than the system-defined locales that are predefined in Cisco IOS software. For example, create the folder for user-defined locale Chinese (User_Define_1) as follows:

TFTP-Root/CME-locale-zh_CN-Chinese-8.6.3.0.tar

Note For a list of user-defined languages supported in Cisco Unified CME, see Cisco Unified CME Localization Matrix.

Table 31: System-Defined and User-Defined Locales

Language	Locale Folder Name	Country Code
English	English_United_States	US
	English_United_Kingdom	UK
		CA
Danish	Danish_Denmark	DK
Dutch	Dutch_Netherlands	NL
French	French_France	FR
		CA

Language	Locale Folder Name	Country Code
German	German_Germany	DE
		AT
		CH
Italian	Italian_Italy	IT
Japanese	Japanese_Japan	JP
Norwegian	Norwegian_Norway	NO
Portuguese	Portuguese_Portugal	PT
Russian	Russian_Russia	RU
Spanish	Spanish_Spain	ES
Swedish	Swedish_Sweden	SE
Un[8]	User_Define_n[1]	Un[1]

8 Where "n" is a number from 1 to 5.

Step 5 Use the **user-locale** [*user-locale-tag*] {[user-defined-code]*country-code*} [**load** *TAR-filename*] command in voice register global configuration mode to extract the contents of the TAR file. For country codes, see Table 31: System-Defined and User-Defined Locales , on page 432.

Note Use the complete filename, including the file suffix (.tar), when you configure the **user-locale** command for all Cisco Unified SIP IP phone types.

Example:

For example, to extract the contents of the CME-locale-zh_CN-Chinese-8.6.3.0.tar file when U1 is the country code for user-defined locale Chinese (User_Define_1), use this command:

```
Router(config-register-global)# user-locale U1 load CME-locale-zh_CN-Chinese-8.6.3.0.tar
```

Step 6 Assign the locales to the phones. See Configure Multiple Locales on SIP Phones, on page 434.

Step 7 Use the **create profile** command in voice register global configuration mode to generate the configuration profile files required for Cisco Unified SIP IP phones.

Step 8 Use the **reset** command to reset the phones and see the localized displays.

Configure Multiple Locales on SIP Phones

To define one or more alternatives to the default user and network locales and apply them to individual phones, perform the following steps.

Restriction

- Multiple user and network locales are supported only on Cisco Unified IP Phone 8961, 9951, and 9971.

Before You Begin

- Cisco Unified CME 8.6 or a later version. For Cisco Unified IP Phone 9971, Cisco Unified CME 8.8 or a later version.
- To specify alternative user and network locales for individual phones in a Cisco Unified CME system, you must use per-phone configuration files. For more information, see Install System-Defined Locales for Cisco Unified IP Phone 6921, 6945, 7906, 7911, 7921, 7931, 7941, 7961, 7970, 7971, and Cisco IP Communicator, on page 411.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **user-locale** [*user-locale-tag*] {[*user-defined-code*] *country-code*}
5. **network-locale** *network-locale-tag* [*user-defined-code*] *country-code*
6. **create profile**
7. **exit**
8. **voice register template** *template-tag*
9. **user-locale** *user-locale-tag*
10. **network-locale** *network-locale-tag*
11. **exit**
12. **voice register pool** *pool-tag*
13. **voice register template** *template-tag*
14. **exit**
15. **voice register global**
16. **reset**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)#voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**user-locale** [*user-locale-tag*] {[*user-defined-code*] *country-code*} **Example:** `Router(config-register-global)# user-locale 1 DE`	Specifies a language for phone displays. • *user-locale-tag*—Assigns a locale identifier to the locale. Range is 0 to 4. Default: 0. This argument is required when defining some locale other than the default (0). • *country-code*—Type **?** to display a list of system-defined codes. Default: US (United States).
Step 5	**network-locale** *network-locale-tag* [*user-defined-code*] *country-code* **Example:** `Router(config-register-global)# network-locale 1 FR`	Specifies a country for tones and cadences. • *network-locale-tag*—Assigns a locale identifier to the country code. Range is 0 to 4. Default: 0. This argument is required when defining some locale other than the default (0). • *country-code*—Type **?** to display a list of system-defined codes. Default: US (United States). You can assign any valid ISO 3166 code to a user-defined code (U1 to U5).
Step 6	**create profile** **Example:** `Router(config-register-global)# create profile`	Generates provisioning files required for SIP phones and writes the file to the location specified with the tftp-path command.
Step 7	**exit** **Example:** `Router(config-telephony)# exit`	Exits voice register global configuration mode.
Step 8	**voice register template** *template-tag* **Example:** `Router(config)voice register template 10`	Enters voice register template configuration mode to define a template of common parameters for SIP phones in Cisco Unified CME. • Range— 1 to 10.
Step 9	**user-locale** *user-locale-tag*	Assigns a user locale to this ephone template.

	Command or Action	Purpose
	Example: `Router(config-ephone-template)# user-locale 2`	• *user-locale-tag*—A locale tag that was created in Step 4, on page 435. Range is 0 to 4.
Step 10	**network-locale** *network-locale-tag* **Example:** `Router(config-ephone-template)# network-locale 2`	Assigns a network locale to this ephone template. • *network-locale-tag*—A locale tag that was created in Step 5, on page 435. Range is 0 to 4.
Step 11	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits voice register template configuration mode.
Step 12	**voice register pool** *pool-tag* **Example:** `Router(config)#voice register pool 5`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 13	**voice register template** *template-tag* **Example:** `Router(config)voice register template 10`	Enters voice register template configuration mode to define a template of common parameters for SIP phones in Cisco Unified CME. • Range— 1 to 10.
Step 14	**exit** **Example:** `Router(config-ephone)# exit`	Exits voice register template configuration mode.
Step 15	**voice register global** **Example:** `Router(config)#voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 16	**reset** **Example:** `Router(config-register-global)# reset`	Performs a complete reboot of all phones or the specified phone, including contacting the DHCP and TFTP servers for the latest configuration information.
Step 17	**end** **Example:** `Router(config-register-global)# end`	Returns to privileged EXEC mode.

Verify Multiple Locales on SIP Phones

Step 1 Use the **show voice register tftp-bind** command to display a list of configuration files that are accessible to IP phones using TFTP, including the dictionary, language, and tone configuration files.

Example:

```
Router#sh voice register tftp-bind
    tftp-server syncinfo.xml url system:/cme/sipphone/syncinfo.xml
    tftp-server SIPDefault.cnf url system:/cme/sipphone/SIPDefault.cnf
    tftp-server softkeyDefault_kpml.xml url system:/cme/sipphone/softkeyDefault_kpml
    .xml
    tftp-server softkeyDefault.xml url system:/cme/sipphone/softkeyDefault.xml
    tftp-server softkey2_kpml.xml url system:/cme/sipphone/softkey2_kpml.xml
    tftp-server softkey2.xml url system:/cme/sipphone/softkey2.xml
    tftp-server featurePolicyDefault.xml url system:/cme/sipphone/featurePolicyDefau
    lt.xml
    tftp-server featurePolicy2.xml url system:/cme/sipphone/featurePolicy2.xml
    tftp-server SEPACA016FDC1BD.cnf.xml url system:/cme/sipphone/SEPACA016FDC1BD.cnf
    .xml
```

Step 2 Use the **show voice register template all** command to check the user locale and network locale settings in each ephone template.

Step 3 Use the **show voice register pool all** command to check that the correct templates are applied to phones.

Step 4 If the configuration file location is not TFTP, use the **debug tftp events** command to see which files Cisco Unified CME is looking for and whether the files are found and opened correctly. There are usually three states (“looking for x file,” “opened x file,” and “finished x file”). The file is found when all three states are displayed. For an external TFTP server, you can use the logs from the TFTP server.

Configuration Examples for Localization

Example for Configuring Multiple User and Network Locales

The following example sets the default locale of 0 to Germany, which defines Germany as the default user and network locale. Germany is used for all phones unless you apply a different locale to individual phones using ephone templates.

```
telephony service
     cnf-file location flash:
     cnf-file perphone
     user-locale 0 DE
     network-locale 0 DE
```

After using the previous commands to define Germany as the default user and network locale, use the following commands to return the default value of 0 to US:

```
telephony service
     no user-locale 0 DE
     no network-locale 0 DE
```

Another way to define Germany as the default user and network locale is to use the following commands:

```
telephony service
     cnf-file location flash:
    cnf-file perphone
     user-locale DE
     network-locale DE
```

After using the previous commands, use the following commands to return the default to US:

```
telephony service
     no user-locale DE
     no network-locale DE
```

The following example defines three alternative locales: JP (Japan), FR (France), and ES (Spain). The default is US for all phones that do not have an alternative applied using ephone templates. In this example, ephone 11 uses JP for its locales, ephone 12 uses FR, ephone 13 uses ES, and ephone 14 uses the default, US.

```
telephony-service
     cnf-file location flash:
     cnf-file perphone
     create cnf-files
     user-locale 1 JP
     user-locale 2 FR
     user-locale 3 ES
     network-locale 1 JP
     network-locale 2 FR
     network-locale 3 ES
     create cnf-files

    ephone-template 1
    user-locale 1
     network-locale 1

    ephone-template 2
     user-locale 2
     network-locale 2

    ephone-template 3
     user-locale 3
     network-locale 3

    ephone 11
     button 1:25
     ephone-template 1

    ephone 12
     button 1:26
     ephone-template 2

    ephone 13
     button 1:27
     ephone-template 3

    ephone 14
    button 1:28
```

Example for Configuring User-Defined Locales

The following example shows user-locale tag 1 assigned to code U1, which is defined as ZH for Traditional Chinese. Traditional Chinese is not predefined in the system so you must download the appropriate XML files to support this language.

In this example, ephone 11 uses Traditional Chinese (ZH) and ephone 12 uses the default, US English. The default is US English for all phones that do not have an alternative applied using ephone templates.

```
telephony-service
   cnf-file location flash:
   cnf-file perphone
```

```
 user-locale 1 U1 ZH
 network-locale 1 U1 CN

ephone-template 2
 user-locale 1
 network-locale 1

ephone 11
 button 1:25
 ephone-template 2

ephone 12
 button 1:26
```

Example for Configuring Chinese as the User-Defined Locale

The following is a sample output from the **user-locale** command when you configure the Chinese language as the user-defined locale in Cisco Unified CME:

```
Router(config-register-global)# user-locale U1 load chinese.pkg
Updating CNF files

LOCALE INSTALLER MESSAGE: VER:1
LOCALE INSTALLER MESSAGE: Langcode:zh
LOCALE INSTALLER MESSAGE: Language:Chinese
LOCALE INSTALLER MESSAGE: Filename: 7905-dictionary.xml
LOCALE INSTALLER MESSAGE: Filename: 7905-font.xml
LOCALE INSTALLER MESSAGE: Filename: 7905-kate.xml
LOCALE INSTALLER MESSAGE: Filename: 7960-tones.xml
LOCALE INSTALLER MESSAGE: Filename: mk-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: td-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: tc-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: 7921-font.dat
LOCALE INSTALLER MESSAGE: Filename: 7921-kate.utf-8.xml
LOCALE INSTALLER MESSAGE: Filename: 7921-kate.xml
LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary.utf-8.xml
LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary.xml
LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary-ext.xml
LOCALE INSTALLER MESSAGE: Filename: 7921-dictionary.xml
LOCALE INSTALLER MESSAGE: Filename: g3-tones.xml
LOCALE INSTALLER MESSAGE: Filename: utf8_tags_file
LOCALE INSTALLER MESSAGE: Filename: tags_file
LOCALE INSTALLER MESSAGE: New Locale configured

Processing file:flash:/its/user_define_1_tags_file

Processing file:flash:/its/user_define_1_utf8_tags_file

CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files updating complete
```

Example for Configuring Swedish as the System-Defined Locale

The following is a sample output from the **user-locale** command when you configure the Swedish language as the system-defined locale in Cisco Unified CME:

```
Router(config-register-global)# user-locale SE load swedish.pkg
Updating CNF files

LOCALE INSTALLER MESSAGE: VER:1
LOCALE INSTALLER MESSAGE: Langcode:se
LOCALE INSTALLER MESSAGE: Language:swedish
LOCALE INSTALLER MESSAGE: Filename: g3-tones.xml
LOCALE INSTALLER MESSAGE: Filename: gp-sccp.jar
```

```
LOCALE INSTALLER MESSAGE: Filename: ipc-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: mk-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: tc-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: td-sccp.jar
LOCALE INSTALLER MESSAGE: New Locale configured

CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files updating complete
```

Configuration Examples for Locale Installer on SCCP Phones

System-Defined Locale is the Default Applied to All Phones

The following example is the output from the **user-locale** command when you configure a system-defined locale for Cisco Unified CME and the locale is on the default locale index (user-locale-tag 0). The *user-locale-tag* argument is required only when using multiple locales; otherwise, the specified language is the default applied to all SCCP phones.

```
Router(config-telephony)# user-locale SE load CME-locale-sv_SV-7.0.1.1a.tar
    Updating CNF files

    LOCALE INSTALLER MESSAGE: VER:1
    LOCALE INSTALLER MESSAGE: Langcode:se
    LOCALE INSTALLER MESSAGE: Language:swedish
    LOCALE INSTALLER MESSAGE: Filename: g3-tones.xml
    LOCALE INSTALLER MESSAGE: Filename: gp-sccp.jar
    LOCALE INSTALLER MESSAGE: Filename: ipc-sccp.jar
    LOCALE INSTALLER MESSAGE: Filename: mk-sccp.jar
    LOCALE INSTALLER MESSAGE: Filename: tc-sccp.jar
    LOCALE INSTALLER MESSAGE: Filename: td-sccp.jar
    LOCALE INSTALLER MESSAGE: New Locale configured

    CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
    CNF files updating complete
    Router(config-telephony)# create cnf-files
    Router(config-telephony)# ephone 3
    Router(config-ephone)# reset
```

User-Defined Locale is Default Language to be Applied to All Phones

The following example is the output from the **user-locale** command when you configure a user-defined locale for Cisco Unified CME and the locale is on the default locale index (user-locale-tag 0). The *user-locale-tag* argument is required when using multiple locales, otherwise the specified language is the default applied to all SCCP phones.

```
Router(config-telephone)# user-locale U1 load CME-locale-xh_CN-7.0.1.1.tar
  Updating CNF files
  LOCALE INSTALLER MESSAGE: VER:1
  LOCALE INSTALLER MESSAGE: Langcode:fi
  LOCALE INSTALLER MESSAGE: Language:Finnish
  LOCALE INSTALLER MESSAGE: Filename: 7905-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: 7905-kate.xml
  LOCALE INSTALLER MESSAGE: Filename: 7920-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-font.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-kate.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-tones.xml
  LOCALE INSTALLER MESSAGE: Filename: mk-sccp.jar
  LOCALE INSTALLER MESSAGE: Filename: tc-sccp.jar
  LOCALE INSTALLER MESSAGE: Filename: td-sccp.jar
```

```
LOCALE INSTALLER MESSAGE: Filename: tags_file
LOCALE INSTALLER MESSAGE: Filename: utf8_tags_file
LOCALE INSTALLER MESSAGE: Filename: g3-tones.xml
LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary.utf-8.xml
LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary.xml
LOCALE INSTALLER MESSAGE: Filename: ipc-sccp.jar
LOCALE INSTALLER MESSAGE: Filename: gp-sccp.jar
LOCALE INSTALLER MESSAGE: New Locale configured

Processing file:flash:/its/user_define_2_tags_file

Processing file:flash:/its/user_define_2_utf8_tags_file

CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files updating complete

Router(config-telephony)# create cnf-files
Router(config-telephony)# ephone 3
Router(config-ephone)# reset
```

Locale on a Non-default Locale Index

The following example is the output from the **user-locale** command if you configure a user-defined locale as an alternate locale for a particular SCCP phone (ephone 1) in Cisco Unified CME. The *user-locale-tag* argument is required only when using multiple locales. In this configuration, the locale is user-defined Finnish (U2) on user-locale index 2.

```
Router(config-telephony)# user-locale 2 U2 load CME-locale-fi_FI-7.0.1.1.tar
  Updating CNF files

  LOCALE INSTALLER MESSAGE: VER:1
  LOCALE INSTALLER MESSAGE: Langcode:fi
  LOCALE INSTALLER MESSAGE: Language:Finnish
  LOCALE INSTALLER MESSAGE: Filename: 7905-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: 7905-kate.xml
  LOCALE INSTALLER MESSAGE: Filename: 7920-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-font.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-kate.xml
  LOCALE INSTALLER MESSAGE: Filename: 7960-tones.xml
  LOCALE INSTALLER MESSAGE: Filename: mk-sccp.jar
  LOCALE INSTALLER MESSAGE: Filename: tc-sccp.jar
  LOCALE INSTALLER MESSAGE: Filename: td-sccp.jar
  LOCALE INSTALLER MESSAGE: Filename: tags_file
  LOCALE INSTALLER MESSAGE: Filename: utf8_tags_file
  LOCALE INSTALLER MESSAGE: Filename: g3-tones.xml
  LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary.utf-8.xml
  LOCALE INSTALLER MESSAGE: Filename: SCCP-dictionary.xml
  LOCALE INSTALLER MESSAGE: Filename: ipc-sccp.jar
  LOCALE INSTALLER MESSAGE: Filename: gp-sccp.jar
  LOCALE INSTALLER MESSAGE: New Locale configured

  Processing file:flash:/its/user_define_2_tags_file

  Processing file:flash:/its/user_define_2_utf8_tags_file

  CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
  CNF files updating complete

  Router(config-telephony)# ephone-template 1
  Router(config-ephone-template)# user-locale 2
  Router(config-ephone-template)# ephone 1
  Router(config-ephone)# ephone-template 1
 The ephone template tag has been changed under this ephone, please restart or reset ephone
to take effect.
  Router(config-ephone)# telephony-service
```

```
Router(config-telephony)# create cnf-files
Router(config-telephony)# ephone 1
Router(config-ephone)# reset
```

Examples for Configuring Multiple User and Network Locales on SIP Phones

The following example sets the default locale of 0 to Germany, which defines Germany as the default user and network locale. Germany is used for all phones unless you apply a different locale to individual phones using ephone templates.

```
voice register global
    user-locale 0 DE
   network-locale 0 DE
```

After using the previous commands to define Germany as the default user and network locale, use the following commands to return the default value of 0 to US:

```
voice register global
   no user-locale 0 DE
  no network-locale 0 DE
```

Another way to define Germany as the default user and network locale is to use the following commands:

```
voice register global
   user-locale DE
   network-locale DE
```

After using the previous commands, use the following commands to return the default to US:

```
voice register global
   no user-locale DE
   no network-locale DE
```

SIP: Alternative Locales

The following example defines three alternative locales: JP (Japan), FR (France), and ES (Spain). The default is US for all phones that do not have an alternative applied using ephone templates. In this example, ephone 11 uses JP for its locales, ephone 12 uses FR, ephone 13 uses ES, and ephone 14 uses the default, US.

```
voice register global
   create profile
   user-locale 1 JP
   user-locale 2 FR
   user-locale 3 ES
   network-locale 1 JP
   network-locale 2 FR
   network-locale 3 ES
   create profile

  voice register template 1
   user-locale 1
   network-locale 1

  voice register template 2
   user-locale 2
   network-locale 2

  voice register pool 1
    number 1 dn 1
    template 1
   user-locale 3
  network-locale 3

  voice register pool 2
    number 2 dn 2
    template 2
```

```
voice register pool 6
  number 3 dn 3
   template 3
```

Example for Configuring Locale Installer on SIP Phones

The following example shows how the locale installer only requires you to copy the locale file using the **copy** command in privileged EXEC configuration mode to configure a locale on a Cisco Unified SIP IP phone. The example also shows that the locale file has been copied in the /its directory.

```
Router# copy tftp://100.1.1.1/CME-locale-de_DE-German-8.6.3.0.tar flash:/its
Destination filename [/its/CME-locale-de_DE-German-8.6.3.0.tar]?
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# voice register global
Router(config-register-global)# user-locale DE load CME-locale-de_DE-German-8.6.3.0.tar
LOCALE INSTALLER MESSAGE (SIP):Loading Locale Package...
LOCALE INSTALLER MESSAGE: VER:3
LOCALE INSTALLER MESSAGE: Langcode:de_DE
LOCALE INSTALLER MESSAGE: Language:German
LOCALE INSTALLER MESSAGE: Filename: g3-tones.xml
LOCALE INSTALLER MESSAGE: Filename: tags_file
LOCALE INSTALLER MESSAGE: Filename: utf8_tags_file
LOCALE INSTALLER MESSAGE: Filename: gd-sip.jar
LOCALE INSTALLER MESSAGE: Filename: gh-sip.jar
LOCALE INSTALLER MESSAGE: Filename: g4-tones.xml
LOCALE INSTALLER MESSAGE: New Locale configured
Router(config-register-global)#
```

Where to Go Next

Ephone Templates

For more information about ephone templates, see Templates, on page 1427.

Feature Information for Localization Support

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

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

Table 32: Feature Information for Localization Support

Feature Name	Cisco Unified CME Version	Feature Information
Localization Enhancements for Cisco Unified SIP IP Phones	10.5	Cisco Unified CME 10.5 provides support for additional languages.

Feature Name	Cisco Unified CME Version	Feature Information
Localization Enhancements for Cisco Unified SIP IP Phones	9.0	Provides the following enhanced localization support for Cisco Unified SIP IP phones: • Localization support for Cisco Unified 6941 and 6945 SIP IP Phones. • Locale installer that supports a single procedure for all Cisco Unified SIP IP phones.
Localization Enhancement	8.8	Adds localization support for Cisco Unified 3905 SIP and Cisco Unified 6945, 8941, and 8945 SCCP IP Phones.
Usability Enhancement	8.6	Adds localization support for SIP IP Phones.
Cisco Unified CME Usability Enhancement	7.0(1)	• Locale installer that supports a single procedure for all SCCP IP phones. • Parses firmware-load text files and automatically creates the required TFTP aliases for localization. • Backward compatibility with the configuration method in Cisco Unified CME 7.0 and earlier versions.
Multiple Locales	4.0	Multiple user and network locales were introduced.
User-Defined Locales	4.0	User-defined locales were introduced.

CHAPTER 12

Dial Plans

This chapter describes features that enable Cisco Unified Communications Manager Express (Cisco Unified CME) to expand or manipulate internal extension numbers so that they conform to numbering plans used by external systems.

Information About Dial Plans

Phone Number Plan

If you install a Cisco Unified CME system to replace an older telephony system that had an established telephone number plan, you can retain the old number plan. Cisco Unified CME supports flexible extension number lengths and can provide automatic conversion between extension dialing and E.164 public telephone number dialing.

When a router receives a voice call, it selects an outbound dial peer by comparing the called number (the full E.164 telephone number) in the call information with the number configured as the destination pattern for the POTS dial peer. The router then strips out the left-justified numbers corresponding to the destination pattern matching the called number. If you have configured a prefix, the prefix will be put in front of the remaining numbers, creating a dial string, which the router will then dial. If all numbers in the destination pattern are stripped-out, the user will receive (depending on the attached equipment) a dial tone.

A successful Cisco Unified CME system requires a telephone numbering plan that supports future expansion. The numbering plan also must not overlap or conflict with other numbers that are on the same VoIP network or are part of a centralized voice mail system.

Cisco Unified CME supports shared lines and multiple lines configured with the same extension number. This means that you can set up several phones to share an extension number to provide coverage for that number. You can also assign several line buttons on a single phone to the same extension number to create a small hunt group.

If you are configuring more than one Cisco Unified CME site, you need to decide how calls between the sites will be handled. Calls between Cisco Unified CME phones can be routed either through the PSTN or over VoIP. If you are routing calls over VoIP, you must decide among the following three choices:

- You can route calls using a global pool of fixed-length extension numbers. For example, all sites have unique extension numbers in the range 5000 to 5999, and routing is managed by a gatekeeper. If you select this method, assign a subrange of extension numbers to each site so that duplicate number assignment does not result. You will have to keep careful records of which Cisco Unified CME system is assigned which number range.
- You can route calls using a local extension number plus a special prefix for each Cisco Unified CME site. This choice allows you to use the same extension numbers at more than one site.
- You can use an E.164 PSTN phone number to route calls over VoIP between Cisco Unified CME sites. In this case, intersite callers use the PSTN area code and local prefix to route calls between Cisco Unified CME systems.

If you choose to have a gatekeeper route calls among multiple Cisco Unified CME systems, you may face additional restrictions on the extension number formats that you use. For example, you might be able to register only PSTN-formatted numbers with the gatekeeper. The gatekeeper might not allow the registration of duplicate telephone numbers in different Cisco Unified CME systems, but you might be able to overcome this limitation. Cisco Unified CME allows the selective registration of either 2- to 5-digit extension numbers or 7- to 10-digit PSTN numbers, so registering only PSTN numbers might prevent the gatekeeper from sensing duplicate extensions.

Mapping of public telephone numbers to internal extension numbers is not restricted to simple truncation of the digit string. Digit substitutions can be made by defining dial plan patterns to be matched. For information about dial plans, see Dial Plan Patterns, on page 446. More sophisticated number manipulations can be managed with voice translation rules and voice translation profiles, which are described in the Voice Translation Rules and Profiles section.

In addition, your selection of a numbering scheme for phones that can be directly dialed from the PSTN is limited by your need to use the range of extensions that are assigned to you by the telephone company that provides your connection to the PSTN. For example, if your telephone company assigns you a range from 408 555-0100 to 408 555-0199, you may assign extension numbers only in the range 100 to 199 if those extensions are going to have Direct Inward Dialing (DID) access. For more information about DID, see Direct Inward Dialing Trunk Lines, on page 447.

Dial Plan Patterns

A dial plan pattern enables abbreviated extensions to be expanded into fully qualified E.164 numbers. Use dial plan patterns when configuring a network with multiple Cisco Unified CMEs to ensure that the appropriate calling number, extension or E.164 number, is provided to the target Cisco Unified CME, and appears on the phone display of the called phone. In networks that have a single router, you do not need to use dial plan patterns.

When you define a directory number for an SCCP phone, the Cisco Unified CME system automatically creates a POTS dial peer with the ephone-dn endpoint as a destination. For SIP phones connected directly into Cisco Unified CME, the dial peer is automatically created when the phone registers. By default, Cisco Unified CME creates a single POTS dial peer for each directory number.

For example, when the ephone-dn with the number 1001 was defined, the following POTS dial peer was automatically created for it:

```
dial-peer voice 20001 pots
 destination-pattern 1001
 voice-port 50/0/2
```

A dial plan pattern builds additional dial peers for the expanded numbers it creates. If a dialplan pattern is configured and it matches against a directory number, two POTS dial peers are created, one for the abbreviated number and one for the complete E.164 direct-dial telephone number.

For example, if you then define a dial plan pattern that 1001 will match, such as 40855500.., a second dial peer is created so that calls to both the 0001 and 4085550001 numbers are completed. In this example, the additional dial peer that is automatically created looks like the following:

```
dial-peer voice 20002 pots
 destination-pattern 40855510001
 voice-port 50/0/2
```

In networks with multiple routers, you may need to use dial plan patterns to expand extensions to E.164 numbers because local extension numbering schemes can overlap each other. Networks with multiple routers have authorities such as gatekeepers that route calls through the network. These authorities require E.164 numbers so that all numbers in the network are unique. Define dial plan patterns to expand extension numbers into unique E.164 numbers for registering with a gatekeeper. For more information on E.164 numbers, see E .164 Enhancements, on page 448.

If multiple dial plan patterns are defined, the system matches extension numbers against the patterns in sequential order, starting with the lowest numbered dial plan pattern tag first. Once a pattern matches an extension number, the pattern is used to generate an expanded number. If additional patterns subsequently match the extension number, they are not used.

Direct Inward Dialing Trunk Lines

Direct Inward Dialing (DID), is a one-way incoming trunking mechanism, that allows an external caller to directly reach a specific extension without the call being served by an attendant or other intervention.

It is a service offered in which the last few (typically three or four) digits dialed by the caller are forwarded to the called party on a special DID trunk. For example, all the phone numbers from 555-0000 to 555-0999 could be assigned to a company with 20 DID trunks. When a caller dials any number in this range, the call is forwarded on any available trunk. If the caller dialed 555-0234, then the digits 2, 3, and 4 are forwarded. These DID trunks could be terminated on a PBX, so that the extension 234 gets the call without operator assistance. This makes it look as though 555-0234 and the other 999 lines all have direct outside lines, while only requiring 20 trunks to service the 1,000 telephone extensions. Using DID, a company can offer its customers individual phone numbers for each person or workstation within the company without requiring a physical line into the PBX for each possible connection. Compared to regular PBX service, DID saves the cost of a switchboard operator. Calls go through faster, and callers feel they are calling a person rather than a company.

Dial plan patterns are required to enable calls to DID numbers. When the PSTN connects a DID call for "4085550234" to the Cisco Unified CME system, it also forwards the extension digits "234" to allow the system to route the call.

Voice Translation Rules and Profiles

Translation rules manipulate dialed numbers to conform to internal or external numbering schemes. Voice translation profiles allow you to group translation rules together and apply them to the following types of numbers:

- Called numbers (DNIS)
- Calling numbers (ANI)
- Redirected called numbers
- Redirected target numbers—These are transfer-to numbers and call-forwarding final destination numbers. Supported by SIP phones in Cisco Unified CME 4.1 and later versions.

After you define a set of translation rules and assign them to a translation profile, you can apply the rules to incoming and outgoing call legs to and from the Cisco Unified CME router based on the directory number. Translation rules can perform regular expression matches and replace substrings. A translation rule replaces a substring of the input number if the number matches the match pattern, number plan, and type present in the rule.

For configuration information, see Define Voice Translation Rules in Cisco CME 3.2 and Later Versions, on page 454.

For examples of voice translation rules and profiles, see the Voice Translation Rules technical note and the Number Translation using Voice Translation Profiles technical note.

Secondary Dial Tone

A secondary dial tone is available for Cisco Unified IP phones connected to Cisco Unified CME. From Cisco Unified CME Release 11.6 onwards, secondary dial tone is supported on both SIP phones and SCCP phones.

The secondary dial tone is generated when a phone user dials a predefined PSTN access prefix and terminates when additional digits are dialed. An example is when a secondary dial tone is heard after a PSTN access prefix, such as the number 9, is dialed to reach an outside line. For SIP phones, a dialplan file is downloaded when the phone restarts. This dialplan file will have the dialplan pattern configured. Based on this dialplan pattern, phone would collect the digits or play secondary dial tone if there is a comma (,) in the pattern. The call is placed from the phone, when there is matching pattern in the dialplan file. Also note that when this feature is enabled, KPML digit collection is disabled on SIP phones.

For configuration information, see Activate Secondary Dial Tone For SCCP Phones, on page 463 and Activate Secondary Dial Tone for SIP Phones, on page 464.

E .164 Enhancements

Cisco Unified CME 8.5 allows you to present a phone number in + E.164 telephone numbering format. E.164 is an International Telecommunication Union (ITU-T) recommendation that defines the international public telecommunication numbering plan used in the PSTN and other data networks. E.164 defines the format of telephone numbers. A leading + E.164 telephone number can have a maximum of 15 digits and is usually written with a '+' prefix defining the international access code. To dial such numbers from a normal fixed line phone, the appropriate international call prefix must be used.

The leading +E.164 number is unique number specified to a phone or a device. Callers from around the world dial the leading + E.164 phone number to reach a phone or a device without the need to know local or international prefix. The leading + E.164 feature also reduces the overall telephony configuration process by eliminating the need to further translate the telephone numbers.

Phone Registration with Leading + E164 Number

In Cisco Unified CME, phones register using the leading '+' dialing plan in two ways. Phones can either register with the extension number or with leading + E.164 number.

When phones are registered with extension number, the phones will have a dial peer association with the extension number. The **dialplan-pattern** command is enhanced to allow you to configure leading + phone numbers on the dialplan pattern. Once dialplan-pattern is configured, there could be an E.164 number dialpeer associated with the same phone.

For example, phones registered with extension number 1111 can also be reached by dialing +13332221111. This phone registration method is beneficial in two ways, that is, locally, phones are able to reach each other by just dialing the extension numbers and, remotely, phones can dial abbreviated numbers which are translated as an E.164 number at the outgoing dial-peer. See Example 1, on page 449 for more information.

Note There are instances where phone is registered with Unified CME using the extension number. If the user has to reach the phone using the full +E.164 number, a dial peer needs to be configured for the full number. This is applicable only when the extension-length is specified to have the same length as extension number.

When phones are registered with a leading + E.164 number, there is only one leading + E.164 number associated with the phone. The **demote** option in the **dialplan-pattern** command allows the phone to have two dialpeers associated with the same phone. For more information on configuring the dialplan-patterns, see Configure Dial Plans, on page 451.

For example, a phone registered with + E.164 phone number +12223331111 will have two dialpeers associated with the same phone that is, +122233331111 and 1111. See Example 2 , on page 450.

Example 1

In the following example, phones are registered with extension number 1111 but they can be reached by either dialing the 4-digit extension number, or a leading + E.164 number (+122233331111). When the dial-peer pattern is configured, phones can also be reached by dialing its + E.164 number. The phone can be reached by dialing either the 4-digit extension number or the + E.164 number.

```
!
ephone-dn 1
 number 1111
!
ephone 1
 button 1:1
!
telephony-service
 dialplan-pattern 1 +1222333.... extension-length 4
!
voice register dn 1
 number 1235
!
voice register pool 1
 number 1 dn 1
!
voice register global
```

```
 dialplan-pattern 1 +1222333.... extension-length 4
```

Example 2

In the following example, phones are registered with leading + E.164 number (+122233331111) and the phones can be reached by dialing either the 4-digit extension number or the + E.164 number. In this example, phone can be reached by dialing 1111 or the +E.164 number.

```
!
ephone-dn 1
 number +12223331111

!
ephone 1
 button 1:1

!
telephony-service
 dialplan-pattern 1 +1222333.... extension-length 4 demote

!
voice register dn 1
 number +12223331235

!
voice register pool 1
 number 1 dn 1

!
voice register global
 dialplan-pattern 1 +1222333.... extension-length 4 demote
```

Note Because the legacy phone does not have a '+' button, you can configure dialplan-pattern or translation profile.

Example 3

In the following example, phones are registered with leading + E.164 number (+12223331111) for SCCP phone and +12223331235 for SIP phone) and the phones can be reached by dialing either the 6-digit number or the + E.164 number. The phone number +12223331234 can be reached by dialing either the 6-digit demoted number or the + E.164 number.

```
!
ephone-dn 1
 number +12223331111

!
ephone 1
 button 1:1
!
telephony-service
 dialplan-pattern 1 +1222333.... extension-length 6 demote

!
voice register dn 1
 number +12223331235

!
voice register pool 1
```

```
 number 1 dn 1
!
voice register global
 dialplan-pattern 1 +1222333.... extension-length 6 demote
```

After the CLI for demote is configured to extension-length 6, you can dial 331235 for SIP phone, and 331111 for SCCP phone.

Callback and Calling Number Display

In earlier versions of Cisco Unified CME and Cisco Unified SRST, the calling number (number from an incoming call ringing on your phone) was used for both callback (number displayed under Missed Calls in your local phone directory number) and calling numbers. The + E.164 feature in Cisco Unified CME 8.5, allows you to display both calling number and callback numbers in appropriate format so that you are not required to edit the phone numbers before placing a call. The calling number is displayed on the phone when you configure the **translation-profile outgoing** command in ephone-dn or voice register dn mode.

The **translate callback-number** configuration in voice translation-profile allows you to translate the callback number and display it in E.164 format. The **translate callback number** configuration is only applicable for outgoing calls on SIP and SCCP IP phones. When **translate callback number** is configured, the extra callback field is displayed and if the number matches the translation rule, it is translated. For more information see Define Translation Rules for Callback-Number on SIP Phones, on page 466.

Similarly, in Cisco Unified SRST 8.5, you can configure **translate calling** under **voice translation-profile** mode to display the calling number. You can configure **translation-profile outgoing** in **call-manager-fallback** mode or **voice register pool** to display the callback number. You can use **translate called** command in **translation-profile** and **call-manager-fallback** or**voice register pool** will try to match the called number to do the translation. See Enabling Translation Profiles for more information.

The leading ‘+’ in the E.164 number is stripped from the called and calling numbers if the called endpoint or gateway, such as H323 or QSIG gateway, does not support the leading ‘+’ sign in the E.164 number translation. You can strip the leading ‘+’ sign from the number you are calling or a called number using the **translation-profile incoming** or **translation-profile outgoing** commands.

Configure Dial Plans

Configure SCCP Dial Plan Patterns

Tip In networks that have a single router, you do not need to define dial plan patterns.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **dialplan-pattern** *tag pattern* **extension-length** *length* [**extension-pattern** *epattern*] [**no-reg**]
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**dialplan-pattern** *tag pattern* **extension-length** *length* [**extension-pattern** *epattern*] [**no-reg**] **Example:** `Router(config-telephony)# 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.	Maps a digit pattern for an abbreviated extension-number prefix to the full E.164 telephone number pattern.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure SIP Dial Plan Patterns

To create and apply a pattern for expanding individual abbreviated SIP extensions into fully qualified E.164 numbers, follow the steps in this section. dial plan pattern expansion affects calling numbers and for call forward using B2BUA, redirecting, including originating and last reroute, numbers for SIP extensions in Cisco Unified CME.

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **dialplan-pattern** *tag pattern* **extension-length** *extension-length* [**extension-pattern** *extension-pattern* | **no-reg**]
5. **call-forward system redirecting-expanded**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**dialplan-pattern** *tag pattern* **extension-length** *extension-length* [**extension-pattern** *extension-pattern* | **no-reg**] **Example:** `Router(config-register-global)# dialplan-pattern 1 4085550... extension-length 5`	Defines pattern that is used to expand abbreviated extension numbers of SIP calling numbers in Cisco Unified CME into fully qualified E.164 numbers.
Step 5	**call-forward system redirecting-expanded** **Example:** `Router(config-register-global)# call-forward system redirecting-expanded`	Applies dial plan pattern expansion globally to redirecting, including originating and last reroute, numbers for SIP extensions in Cisco Unified CME for call forward using B2BUA.
Step 6	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

Verify Dial Plan Patterns

SUMMARY STEPS

1. **show telephony-service**
2. SCCP: **show telephony-service dial-peer** or SIP: **show dial-peer summary**

DETAILED STEPS

Step 1 **show telephony-service**
Use this command to verify dial plan patterns in the configuration.

Example:
The following example maps the extension pattern 4.. to the last three digits of the dial plan pattern 4085550155:

```
telephony-service
 dialplan-pattern 1 4085550155 extension-length 3 extension-pattern 4..
```

Step 2 SCCP: **show telephony-service dial-peer** or SIP: **show dial-peer summary**
Use the command to display dial peers that are automatically created by the **dialplan-pattern** command.

Use this command display the configuration for all VoIP and POTS dial peers configured for a router, including dial peers created by using the **dialplan-expansion (voice register)** command.

Example:
The following example is output from the **show dial-peer summary** command displaying information for four dial peers, one each for extensions 60001 and 60002 and because the **dialplan-expansion** command is configured to expand 6.... to 4085555...., one each for 4085550001 and 4085550002. The latter two dial peers will not appear in the running configuration.

```
Router# show dial-peer summary
             AD                                   PRE  PASS                 OUT
TAG     TYPE  MIN   OPER PREFIX     DEST-PATTERN       FER THRU SESS-TARGET     STATT
20010   pots  up    up              60002$              0                        0
20011   pots  up    up              60001$              0                        9
20012   pots  up    up              5105555001$         0                        9
20013   pots  up    up              5105555002$         0                        0
```

Define Voice Translation Rules in Cisco CME 3.2 and Later Versions

Note To configure translation rules for voice calls in Cisco CME 3.1 and earlier versions, see Cisco IOS Voice, Video, and FAX Configuration Guide.

Before You Begin

- SCCP support—Cisco CME 3.2 or a later version.

- SIP support—Cisco Unified CME 4.1 or a later version.
- To define up to 100 translation rules per translation rule table—Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice translation-rule** *number*
4. **rule** *precedence /match-pattern/ /replace-pattern/*
5. **exit**
6. **voice translation-profile** *name*
7. **translate** {**called** | **calling**| **redirect-called** | **redirect-target**} *translation-rule-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 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: 1 to 2147483647.
Step 4	**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: 1 to 100. **Note** Range limited to 15 maximum rules in CME 8.5 and earlier versions. • *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.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(cfg-translation-rule)# exit`	Exits voice translation-rule configuration mode.
Step 6	**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 7	**translate** {**called** | **calling**| **redirect-called** | **redirect-target**} *translation-rule-number* **Example:** `Router(cfg-translation-profile)# translate called 1`	Associates a 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. • **redirect-target—**Associates the translation rule with transfer-to numbers and call-forwarding final destination numbers. This keyword is supported by SIP phones in Cisco Unified CME 4.1 and later versions. • *translation-rule-number*—Reference number of the translation rule configured in Step 3, on page 455. Range: 1 to 2147483647.
Step 8	**end** **Example:** `Router(cfg-translation-profile)# end`	Returns to privileged EXEC mode.

What to Do Next

- To apply voice translation profiles to SCCP phones connected to Cisco Unified CME 3.2 or a later version, see Apply Voice Translation Rules on SCCP Phones in Cisco Unified CME 3.2 and Later Versions, on page 457.
- To apply voice translation profiles to SIP phones connected to Cisco Unified CME 4.1 or a later version, see Apply Voice Translation Rules on SIP Phones in Cisco Unified CME 4.1 and Later, on page 459.
- To apply voice translation profiles to SIP phones connected to Cisco CME 3.4 or Cisco Unified CME 4.0(x), see Apply Voice Translation Rules on SIP Phones Before Cisco Unified CME 4.1, on page 460.

Apply Voice Translation Rules on SCCP Phones in Cisco Unified CME 3.2 and Later Versions

To apply a voice translation profile to incoming or outgoing calls to or from a directory number on a SCCP phone, perform the following steps.

Before You Begin

- Cisco CME 3.2 or a later version.
- Voice translation profile containing voice translation rules to be applied must be already configured. For configuration information, see Define Voice Translation Rules in Cisco CME 3.2 and Later Versions, on page 454.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *tag*
4. **translation-profile** {**incoming** | **outgoing**} *name*
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-dn** *tag* **Example:** `Router(config)# ephone-dn 1`	Enters ephone-dn configuration mode to create an extension (ephone-dn) for a Cisco Unified IP phone line, an intercom line, a paging line, a voice-mail port, or a message-waiting indicator (MWI). • *tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. Range is 1 to the maximum number of ephone-dns allowed on the router platform. See the CLI help for the maximum value for this argument.
Step 4	**translation-profile** {**incoming** | **outgoing**} *name*	Assigns a translation profile for incoming or outgoing call legs to or from Cisco Unified IP phones.

	Command or Action	Purpose
	Example: `Router(config-ephone-dn)# translation-profile outgoing name1`	• You can also use an ephone-dn template to apply this command to one or more directory numbers. If you use an ephone-dn template to apply a command and you use the same command in ephone-dn configuration mode for the same directory number, the value that you set in ephone-dn configuration mode has priority.
Step 5	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Apply Translation Rules on SCCP Phones Before Cisco Unified CME 3.2

To apply a translation rule to an individual directory number in Cisco CME 3.1 and earlier versions, perform the following steps.

Before You Begin

Translation rule to be applied must be already configured by using the **translation-rule** and **rule** commands. For configuration information, see Cisco IOS Voice, Video, and FAX Configuration Guide.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *tag*
4. **translate** {**called** | **calling**} *translation-rule-tag*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *tag* **Example:** `Router(config)# ephone-dn 1`	Enters ephone-dn configuration mode to create directory number for a Cisco Unified IP phone line, an intercom line, a paging line, a voice-mail port, or a message-waiting indicator (MWI).
Step 4	**translate** {**called** | **calling**} *translation-rule-tag* **Example:** `Router(config-ephone-dn)# translate called 1`	Specifies rule to be applied to the directory number being configured. • *translation-rule-tag*—Reference number of previously configured translation rule. Range: 1 to 2147483647. • You can use an ephone-dn template to apply this command to one or more directory numbers. If you use an ephone-dn template to apply a command to a directory number and you also use the same command in ephone-dn configuration mode for the same directory number, the value that you set in ephone-dn configuration mode has priority.
Step 5	**end** **Example:** `Router(cfg-translation-profile)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Apply Voice Translation Rules on SIP Phones in Cisco Unified CME 4.1 and Later

To apply a voice translation profile to incoming calls to a directory number on a SIP phone, perform the following steps.

Before You Begin

- Cisco Unified CME 4.1 or a later version.
- Voice translation profile containing voice translation rules to be applied must be already configured. For configuration information, see Define Voice Translation Rules in Cisco CME 3.2 and Later Versions, on page 454.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **translation-profile incoming** *name*
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 register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI).
Step 4	**translation-profile incoming** *name* **Example:** `Router(config-register-dn)# translation-profile incoming name1`	Assigns a translation profile for incoming call legs to this directory number.
Step 5	**end** **Example:** `Router(config-register-dn)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Apply Voice Translation Rules on SIP Phones Before Cisco Unified CME 4.1

To apply an already-configured voice translation rule to modify the number dialed by extensions on a SIP phone, perform the following steps.

Before You Begin

- Cisco CME 3.4 or a later version.
- Voice translation rule to be applied must be already configured. For configuration information, see Define Voice Translation Rules in Cisco CME 3.2 and Later Versions, on page 454.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **translate-outgoing** {**called** | **calling**} *rule-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	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for SIP phones.
Step 4	**translate-outgoing** {**called** | **calling**} *rule-tag* **Example:** `Router(config-register-pool)# translate-outgoing called 1`	Specifies an already configured voice translation rule to be applied to SIP phone being configured.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Verify Voice Translation Rules and Profiles

To verify voice translation profiles, and rules, perform the following steps.

SUMMARY STEPS

1. **show voice translation-profile** [*name*]
2. **show voice translation-rule** [*number*]
3. **test voice translation-rule** *number*

DETAILED STEPS

Step 1 **show voice translation-profile** [*name*]
This command displays the configuration of one or all translation profiles.

Example:

```
Router# show voice translation-profile profile-8415

Translation Profile: profile-8415
  Rule for Calling number: 4
  Rule for Called number: 1
  Rule for Redirect number: 5
  Rule for Redirect-target number: 2
```

Step 2 **show voice translation-rule** [*number*]
This command displays the configuration of one or all translation rules.

Example:

```
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 3 **test voice translation-rule** *number*
This command enables you to test your translation rules.

Example:

```
Router(config)# voice translation-rule 5
Router(cfg-translation-rule)# rule 1 /201/ /102/
Router(cfg-translation-rule)# exit
Router(config)# exit
```

```
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
```

Activate Secondary Dial Tone For SCCP Phones

To activate a secondary dial tone after a phone user dials the specified number, perform the following steps.

Before You Begin

- Cisco CME 3.0 or a later version.
- PSTN access prefix must be configured for outbound dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **secondary-dialtone** *digit-string*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**secondary-dialtone** *digit-string*	Activates a secondary dial tone when *digit-string* is dialed.

	Command or Action	Purpose
	Example: `Router(config-telephony)#` **secondary-dialtone 9**	• *digit-string*—String of up to 32 digits that, when dialed, activates a secondary dial tone. Typically, the *digit-string* is a predefined PSTN access prefix.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Activate Secondary Dial Tone for SIP Phones

To activate a secondary dial tone after a phone user dials the specified number, perform the following steps.

Before You Begin

- Cisco Unified CME 11.6 or later for SIP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dialplan** *tag*
4. **type** *7940-7960-others*
5. **pattern tag** *string*
6. **voice register pool** *tag*
7. **dialplan** *tag*
8. **voice register global**
9. **create profile**
10. **voice register pool** *tag*
11. **reset**
12. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register dialplan** *tag* **Example:** `Router(config)# voice register dialplan 1`	Enters voice register dialplan configuration mode. • *tag*—Range for dialplan tag is 1 to 24.
Step 4	**type** *7940-7960-others* **Example:** `Router(config-register-dialplan)# type 7940-7960-others`	Specifies the phone type assigned.
Step 5	**pattern tag** *string* **Example:** `Router(config-register-dialplan)# pattern 1 30,`	Specifies the pattern to be matched while dialing from phone. Range is 1 to 24. • *tag*—Range for pattern tag is 1 to 24. • *string*—It is the pattern to be matched while dialing from phone. This string is represented as WORD and the value of this string can be a combination of [0-9.*#,].
Step 6	**voice register pool** *tag* **Example:** `Router(config-register-dialplan)# voice register pool 1`	Defines the voice register pool tag, and enters the voice register pool configuration mode.
Step 7	**dialplan** *tag* **Example:** `Router(config-register-pool)# dialplan 1`	Specifies the dialplan to be attached to the pool.
Step 8	**voice register global** **Example:** `Router(config-register-pool)# voice register global`	Enters voice register global configuration mode.
Step 9	**create profile** **Example:** `Router(config-register-global)# create profile`	Creates the XML configuration files for the phone.

	Command or Action	Purpose
Step 10	**voice register pool** *tag* **Example:** `Router(config-register-global)# voice register pool 1`	Defines the voice register pool tag, and enters the voice register pool configuration mode.
Step 11	**reset** **Example:** `Router(config-register-pool)# reset`	Resets the phone for the phone configurations to be applied.
Step 12	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Define Translation Rules for Callback-Number on SIP Phones

Before You Begin

- To define up to 100 translation rules per translation rule table—Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice translation-rule** *number*
4. **rule** *precedence* | *match-pattern* | *replace-pattern*|
5. **exit**
6. **voice translation-profile** *name*
7. **translate** {**callback-number** | **called** | **calling** | **redirect-called** | **redirect-target**} **translation-rule**-*number*
8. **exit**
9. **voice register pool** *phone-tag*
10. **number** *tag* **dn** *dn-tag*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice translation-rule** *number* **Example:** `Router(config)# voice translation-rule 10`	Defines a translation rule for voice calls and enters voice translation-rule configuration mode. • *number*—Number that identifies the translation rule. Range: 1 to 2147483647.
Step 4	**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: 1 to 100. **Note** Range limited to 15 maximum rules in CME 8.5 and earlier versions. • *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 5	**exit** **Example:** `Router(cfg-translation-rule)# exit`	Exits voice translation-rule configuration mode.
Step 6	**voice translation-profile** *name* **Example:** `Router(config)# voice translation-profile eastern`	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 7	**translate** {**callback-number** | **called** | **calling** | **redirect-called** | **redirect-target**} **translation-rule**-*number* **Example:** `Router(cfg-translation-profile)# translate callback-number 10`	Associates a translation rule with a voice translation profile. • callback-number—Associates the translation rule with the callback-number. • 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.

	Command or Action	Purpose
		• redirect-target—Associates the translation rule with transfer-to numbers and call-forwarding final destination numbers. This keyword is supported by SIP phones in Cisco Unified CME 4.1 and later versions. • translation-rule-*number*—Reference number of the translation rule configured in Step 3, on page 467. Range: 1 to 2147483647
Step 8	**exit** **Example:** `Router(cfg-translation-profile))# exit`	Exits voice translation-profile configuration mode.
Step 9	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 3`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 10	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 17`	Associates a directory number with the SIP phone being configured. • **dn** *dn-tag*—identifies the directory number for this SIP phone as defined by the voice register dn command.
Step 11	**end** **Example:** `Router(config-translation-profile)# end`	Returns to privileged EXEC mode.

The following examples show translation rules defined for callback-number:

```
!
!
voice service voip
ip address trusted list
  ipv4 20.20.20.1
 media flow-around
 allow-connections sip to sip
!
!
voice translation-rule 10
!
!
voice translation-profile eastcoast
!
voice translation-profile eastern
 translate callback-number 10
!
```

What to Do Next

- To apply voice translation profiles to SIP phones connected to Cisco Unified CME 4.1 or a later version, see Apply Voice Translation Rules on SIP Phones in Cisco Unified CME 4.1 and Later, on page 459.

Configuration Examples for Dial Plan Features

Example for Configuring Secondary Dial Tone on SCCP Phones

```
telephony-service
  fxo hook-flash
  load 7910 P00403020214
  load 7960-7940 P00305000600
  load 7914 S00103020002
  load 7905 CP7905040000SCCP040701A
  load 7912 CP7912040000SCCP040701A
  max-ephones 100
  max-dn 500
  ip source-address 10.153.233.41 port 2000
  max-redirect 20
  no service directed-pickup
  timeouts ringing 10
  system message XYZ Company
  voicemail 7189
  max-conferences 8 gain -6
  moh music-on-hold.au
  web admin system name admin1 password admin1
  dn-webedit
  time-webedit
  !
  !
  !
  secondary-dialtone 9
```

Example for Configuring Secondary Dial Tone on SIP Phones

A secondary dial tone is played on the phone when comma (',') is found in the pattern. In this example, secondary dial tone is played after the digit 50.

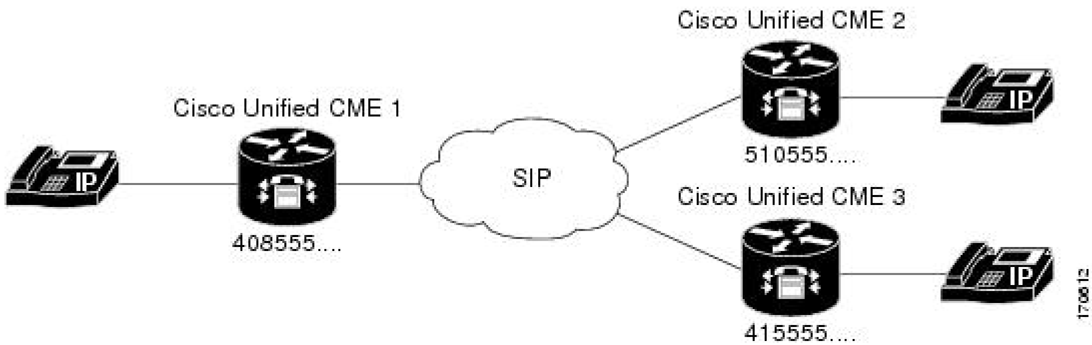
```
voice register dialplan 1
 type 7940-7960-others
 pattern 1 50,

voice register pool 1
 busy-trigger-per-button 2
 id mac 0C11.6780.52A3
 type 7841
number 1 dn 1
 dialplan 1
 dtmf-relay rtp-nte
 username cisco1 password cisco
 codec g711ulaw
 no vad
 provision-tag 1
```

Example for Configuring Voice Translation Rules

In the following configuration examples, if a user on Cisco Unified CME 1 dials 94155550100, the call matches on dial peer 9415 and uses translation profile *profile-9415*. The called number is translated from 94155550100 to 4155550100, as specified by the **translate called** command using translation rule 1.

If a user on Cisco Unified CME 1 calls a phone on Cisco Unified CME 2 by dialing 5105550120, and the call forward number is 94155550100, Cisco Unified CME 1 attempts to forward the call to 94155550100. A 302 message is then sent to Cisco Unified CME 1 with the "Contact:" field translated to 4155550100. When the 302 reaches Cisco Unified CME 1, it matches the To: field in the 302 message (5105550120) with dial peer 510. It does incoming translation from 4155550100 to 84155550100, and an INVITE with 84155550100 is sent, which matches dial-peer 8415.

Figure 14: Translation Rules in SIP Call Transfer



Cisco Unified CME 1 with 408555.... dialplan-pattern	Cisco Unified CME 2 with 510555.... dialplan-pattern
dial-peer voice 9415 voip translation-profile outgoing profile-9415 destination-pattern 9415555.... session protocol sipv2 session target ipv4:10.4.187.177 codec g711ulaw voice translation-profile profile-9415 translate called 1 translate redirect-target 1 voice translation-rule 1 rule 1 /^9415/ /415/	dial-peer voice 8415 voip translation-profile outgoing profile-8415 destination-pattern 8415555.... session protocol sipv2 session target ipv4:10.4.187.177 codec g711ulaw dial-peer voice 510 voip translation-profile incoming profile-510 destination-pattern 510555.... session protocol sipv2 session target ipv4:10.4.187.188 codec g711ulaw voice translation-profile profile-8415 translate called 1 translate redirect-target 2 voice translation-profile profile-510 translate called 3 voice translation-rule 1 rule 1 /^9415/ /415/ voice translation-rule 2 rule 2 /^415/ /9415/ voice translation-rule 3 rule 1 /^8415/ /415/

Feature Information for Dial Plan Features

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

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

Table 33: Feature Information for Dialing Plan Features

Feature Name	Cisco Unified CME Versions	Feature Information
Dial Plan Pattern	4.0	Added support for dial plan pattern expansion for call forward and call transfer when the forward or transfer-to target is an individual abbreviated SIP extension or an extension that appear on a SIP phone.
	2.1	Strips leading digit pattern from extension number when expanding an extension to an E.164 telephone number. The length of the extension pattern must equal the value configured for the extension-length argument.
	1.0	Adds a prefix to extensions to transform them into E.164 numbers.
E.164 Enhancements	8.5	Added support for E.164 enhancements.
Secondary Dial Tone	11.6	Support for Secondary Dial Tone on SIP phones.
	3.0	Support for secondary dial tone after dialing specified number string.

Feature Name	Cisco Unified CME Versions	Feature Information
Voice Translation Rules	8.6	Added support for an increased number of translation rules per translaiton table. Old value is 15 maximum, new value is 100 maximum.
	4.1	Added support for voice translation profiles for incoming call legs to a directory number on a SIP phone.
	3.4	Added support for voice translation rules to modify the number dialed by extensions on a SIP phone.
	3.2	Adds, removes, or transforms digits for calls going to or originating from specified ephone-dns.

CHAPTER 13

Transcoding Resources

This chapter describes the transcoding support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Note

- To configure a DSP farm profile for multi-party ad hoc and meet-me conferencing in Cisco Unified CME 4.1 and later versions, see Meet-Me Conferencing in Cisco Unified CME 4.1 and Later versions, on page 1373 and Meet-Me Conferencing in Cisco Unified CME 11.7 and Later Versions, on page 1374.
- To configure DSP farms for meet-me conferencing in Cisco CME 3.2 to Cisco Unified CME 4.0. see Meet-Me Conferencing in Cisco CME 3.2 to Cisco Unified CME 4.0, on page 1375.

Prerequisites for Configuring Transcoding Resources

- Cisco Unified CME 3.2 or a later version.
- Cisco Unified CME 11.6 or later versions for LTI-based transcoding, supported on Cisco 4000 Series Integrated Services Router (ISR).

Restrictions for Configuring Transcoding Resources

- Before Cisco CME 3.2, only G.729 is supported for two-party voice calls.
- In Cisco CME 3.2 to Cisco Unified CME 4.0, transcoding between G.711 and G.729 does not support the following:
    - Meet-me conferencing
    - Multiple-party ad-hoc conferencing
    - Transcoding security
- For Cisco Unified CME Release 11.6, hardware conferencing is not supported with LTI-based transcoding on Cisco 4000 Series Integrated Services Router (ISR).
- In Unified CME 11.6, SCCP based transcoding is not supported.

Information About Transcoding Resources

Transcoding Support

Transcoding compresses and decompresses voice streams to match endpoint-device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth, and the local device does not support that type of compression.

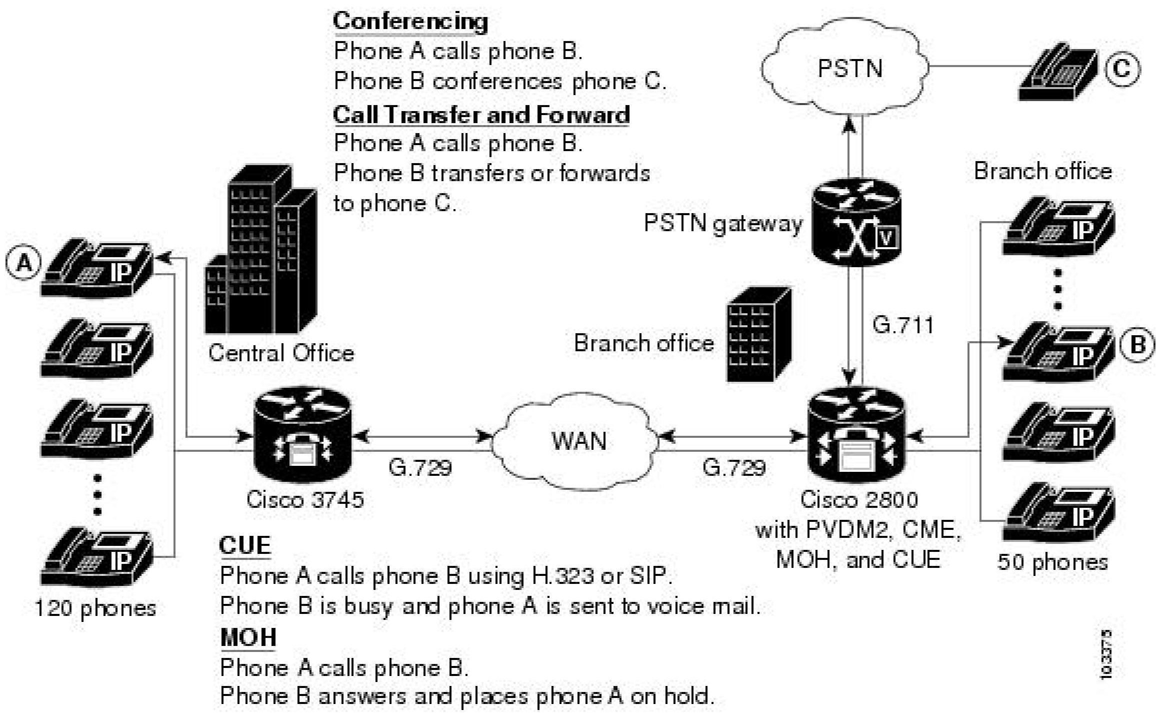
Cisco Unified CME 3.2 and later versions support transcoding between G.711 and G.729 codecs for the following features:

- Ad hoc conferencing—One or more remote conferencing parties uses G.729.
- Call transfer and forward—One leg of a Voice over IP (VoIP)-to-VoIP hairpin call uses G.711 and the other leg uses G.729. A hairpin call is an incoming call that is transferred or forwarded over the same interface from which it arrived.
- Cisco Unity Express or Cisco Unity Express Virtual—An H.323 or SIP call using G.729 is forwarded to Cisco Unity Express or Cisco Unity Express Virtual. Cisco Unity Express or Cisco Unity Express Virtual supports only G.711, so G.729 must be transcoded.

  From Cisco Unified CME Release 11.6 onwards, SIP calls coming to Cisco Unity Express or Cisco Unity Express Virtual is supported on Cisco 4000 Series ISR routers using the LTI transcoding infrastructure. For more information on configuring LTI transcoding on Cisco Unified CME, see Configure LTI-based Transcoding, on page 506.
- Music on hold (MOH)—The phone receiving MOH is part of a system that uses G.729, G.722, or internet Low Bitrate Codec (iLBC). When the G.711 MOH is transcoded into G.729, it results in a poorer quality sound due to the lower compression of G.729. From Cisco Unified CME Release 11.7 onwards, Music on Hold is supported on Cisco 4000 Series ISR routers using the LTI transcoding infrastructure. For more information on configuring LTI transcoding on Cisco Unified CME, see Configure LTI-based Transcoding, on page 506.

Each of the preceding call situations is illustrated in Figure 15: Three-Way Conferencing, Call Transfer and Forward, Cisco Unity Express, and MOH Between G.711 and G.729, on page 475.

Figure 15: Three-Way Conferencing, Call Transfer and Forward, Cisco Unity Express, and MOH Between G.711 and G.729



Transcoding is facilitated through DSPs, which are located in network modules. All network modules have single in-line memory module (SIMM) sockets or packet voice/data modules (PVDM) slots that each hold a Packet Voice DSP Module (PVDM). Each PVDM holds DSPs. A router can have multiple network modules.

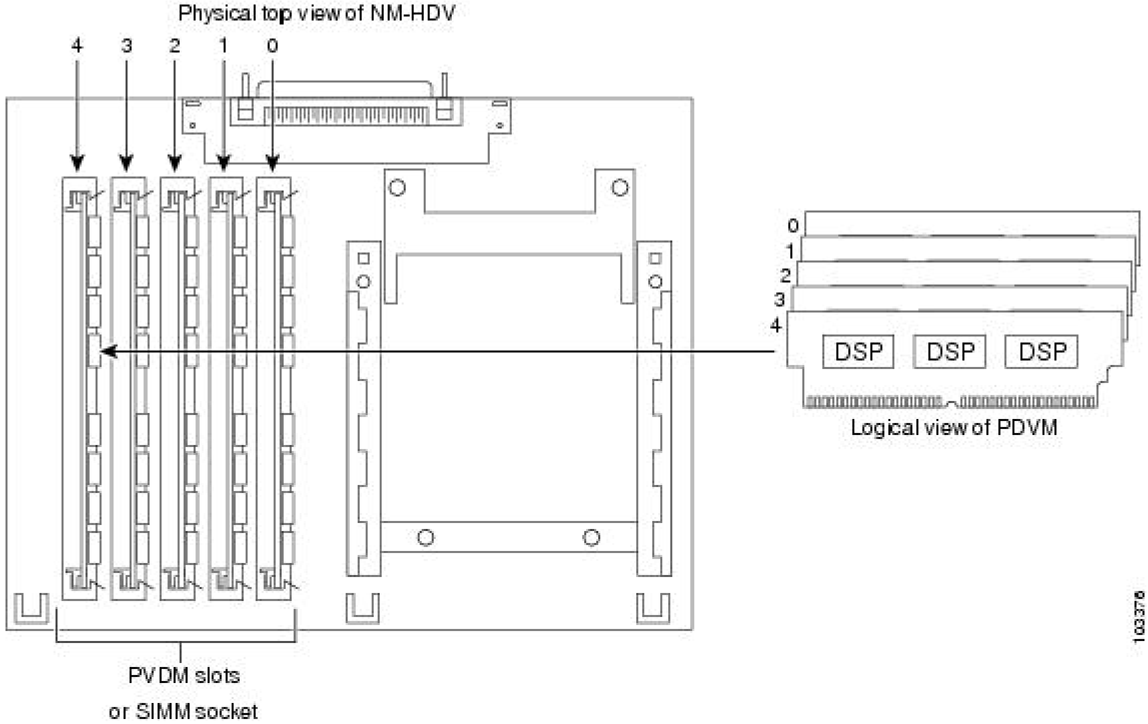
Cisco Unified CME routers and external voice routers on the same LAN must be configured with digital signal processors (DSPs) that support transcoding. DSPs reside either directly on a voice network module, such as the NM-HD-2VE, on PVDM2s that are installed in a voice network module, such as the NM-HDV2, or on PVDM2s that are installed directly onto the motherboard, such as on the Cisco 2800 and 3800 series voice gateway routers.

- DSPs on the NM-HDV, NM-HDV2, NM-HD-1V, NM-HD-2V, and NM-HD-2VE can be configured for transcoding.
- PVDM2-xx on the Cisco 2800 series and the Cisco 3800 series motherboards can also be configured for transcoding.

Transcoding of G.729 calls to G.711 allows G.729 calls to participate in existing G.711 software-based, three-party conferencing, thus eliminating the need to divide DSPs between transcoding and conferencing.

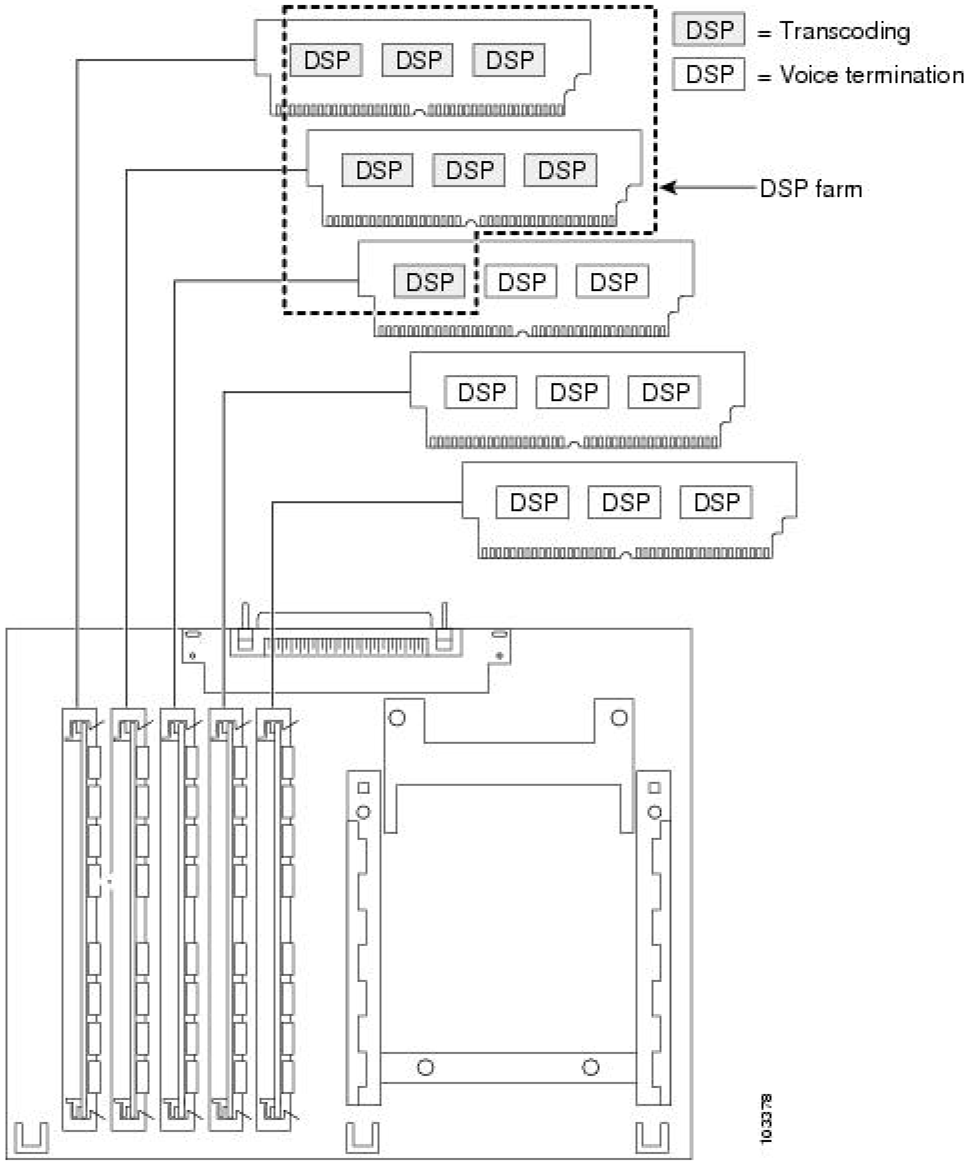
Figure 16: NM-HDV Supports up to Five PVDMs, on page 476 shows an NM-HDV with five SIMM sockets or PVDM slots that each hold a 12-Channel PVDM (PVDM-12). Each PVDM-12 holds three TI 549 DSPs. Each DSP supports four channels.

Figure 16: NM-HDV Supports up to Five PVDMs



Use DSP resources to provide voice termination of the digital voice trunk group or resources for a DSP farm. DSP resources available for transcoding and not used for voice termination are referred to as a DSP farm. Figure 17: DSP Farm, on page 477 shows a DSP farm managed by Cisco Unified CME.

Figure 17: DSP Farm



Local Transcoding Interface (LTI) Based Transcoding

From Cisco Unified CME Release 11.6 onwards, Local Transcoding Interface (LTI) based transcoding is supported on Cisco 4000 series ISR. LTI includes an internal API that accesses digital signal processor (DSP) resources. This API does not require the use of Skinny Client Control Protocol (SCCP) based configuration for transcoding to work.

LTI-based transcoding is an alternative to SCCP-based transcoding. The LTI-based transcoding configures transcoding functionality only on the specific Unified CME router. Unlike the SCCP-based transcoding, other Unified CME routers cannot leverage the transcoding capabilities configured on a specific Unified CME router. That is, transcoding resources (DSPFARM) are required to be co-located with Unified CME router for LTI-based configuration to work. When both LTI-based and SCCP-based transcoding are configured, LTI takes precedence.

With LTI-based transcoding, internal APIs are used to access DSP resources for transcoding. The TCP sockets are not opened and no registration is used. Also, you need to configure only the DSPFARM profile configuration.

Voice Class Codec (VCC) is supported with LTI-based Transcoding on Cisco 4000 Series ISR, and is an optional configuration. A VCC defines the codec preference order. When a voice class codec is applied to a dial peer, the preference order defined in the voice class codec is followed.

LTI infrastructure supports the features SIP-to-SIP line to trunk transcoding, DTMF Interworking (with in-band on the trunk and rtp-nte on the line), and mid-call transcoder invocation and deletion with call transfer. Features such as Shared Line, Call Park, Call Pickup, iDivert, and so on are not supported with LTI-based transcoding.

Transcoding When a Remote Phone Uses G.729r8

A situation in which transcoding resources may be used is when you use the **codec** command to select the G.729r8 codec to help save network bandwidth for a remote IP phone. If a conference is initiated, all phones in the conference switch to G.711 mu-law. To allow the phone to retain its G.729r8 codec setting when joined to a conference, you can use the **codec g729r8 dspfarm-assist** command to specify that this phone’s calls should use the resources of a DSP farm for transcoding. For example, there are two remote phones (A and B) and a local phone (C) that initiates a conference with them. Both A and B are configured to use the G.729r8 codec with the assistance of the DSP-farm transcoder. In the conference, the call leg from C to the conference uses the G.711 mu-law codec, and the call legs from A and B to the Cisco Unified CME router use the G.729r8 codec.

Consider your options carefully when deciding to use the **codec g729r8 dspfarm-assist** command. The benefit is that it allows calls to use the G.729r8 codec on the call leg between the IP phone and the Cisco Unified CME router, which saves network bandwidth. The disadvantage is that for situations requiring G.711 codecs, such as conferencing and Cisco Unity Express, DSP resources that are possibly scarce are used to transcode the call, and delay is introduced while voice is shuttled to and from the DSP. In addition, the overuse of this feature can mask configuration errors in the codec selection mechanisms involving dial peers and codec lists.

Therefore, we recommend using the **codec g729r8 dspfarm-assist** command sparingly and only when absolutely required for bandwidth savings or when you know the phone will be participating very little, if at all, in calls that require a G.711 codec.

Because of how Cisco Unified CME uses voice channels with Skinny Client Control Protocol (SCCP) endpoints, you must configure at least two available transcoding sessions when establishing a call that requires transcoding configured with the **codec g729r8** dspfarm-assist command. Only one session is used after the voice path is established with transcoding. However, during the SCCP manipulations, a temporary session may be allocated. If this temporary session cannot be allocated, the transcoding request is not honored, and the call continues with the G.711 codec.

If the **codec g729r8 dspfarm-assist** command is configured for a phone and a DSP resource is not available when needed for transcoding, a phone registered to the local Cisco Unified CME router will use G.711 instead of G.729r8. This is not true for nonSCCP call legs; if DSP resources are not available for the transcoding required for a conference, for example, the conference is not created.

Secure DSP Farm Transcoding

Cisco Unified CME uses the secure transcoding DSP farm capability only in the case described in Transcoding When a Remote Phone Uses G.729r8, on page 478. If a call using the **codec g729r8 dspfarm-assist** command is secure, Cisco Unified CME looks for a secure transcoding resource. If it cannot find one, transcoding is not done. If the call is not secure, Cisco Unified CME looks for a nonsecure transcoding resource. If it cannot find one, Cisco Unified CME looks for a secure transcoding resource. Even if Cisco Unified CME uses a secure transcoding resource, the call is not secure, and a more expensive secure DSP Farm resource is not needed for a nonsecure call because Cisco Unified CME cannot find a less expensive nonsecure transcoder.

Configure Transcoding Resources

This section contains the following tasks:

Determine DSP Resource Requirements for Transcoding

To determine if that there are enough DSPs available on your router for transcoding services, perform the following steps.

Step 1 Use the **show voice dsp** command to display current status of digital signal processor (DSP) voice channels.

Step 2 Use the **show sdspfarm sessions** command to display the number of transcoder sessions that are active.

Step 3 Use the **show sdspfarm units** command to display the number of DSP farms that are configured.

Provision Network Modules or PVDMs for Transcoding

DSPs can reside directly on any one of the following:

- A voice network module, such as the NM-HD-2VE,
- PVDM2s that are installed in a voice network module, such as the NM-HDV2. A single network module can hold up to five PVDMs.
- PVDM2s that are installed directly onto the motherboard, such as on the Cisco 2800 and 3800 series voice gateway routers.

You must determine the number of PVDM2s or network modules that are required to support your conferencing and transcoding services and install the modules on your router.

SUMMARY STEPS

1. Determine performance requirements.
2. Determine the number of DSPs that are required.
3. Determine the number of DSPs that are supportable

4 Verify your solution.

5 Install hardware.

DETAILED STEPS

Step 1 Determine the number of transcoding sessions that your router must support.

Step 2 Determine the number of DSPs that are required to support transcoding sessions. See Table 5 and Table 6 in the "Allocation of DSP Resources" section of the "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" chapter of the Cisco Unified Communications Manager and Cisco IOS Interoperability Guide.
If voice termination is also required, determine the additional number of DSPs required.

For example: 16 transcoding sessions (30-ms packetization) and 4 G.711 voice calls require two DSPs.

Step 3 Determine the maximum number of NMs or NM farms that your router can support by using Table 4 in the "Allocation of DSP Resources" section of the "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" chapter of the Cisco Unified Communications Manager and Cisco IOS Interoperability Guide.

Step 4 Ensure that your requirements fall within router capabilities, taking into account whether your router supports multiple NMs or NM farms. If necessary, reassess performance requirement.

Step 5 Install PVDMs, NMs, and NM farms as needed. See the Connecting Voice Network Modules chapter in the *Cisco Network Modules Hardware Installation Guide*.

What to Do Next

Perform one of the following options, depending on the type of network module to be configured:

- To set up DSP farms on NM-HDs and NM-HDV2s, see Configure DSP Farms for NM-HDs and NM-HDV2s, on page 481.
- To set up DSP farms for NM-HDVs, see Configure DSP Farms for NM-HDVs, on page 485.

Configure DSP Farms for NM-HDs and NM-HDV2s

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dsp services dspfarm**
5. **exit**
6. **sccp local** *interface-type interface-number*
7. **sccp ccm** *ip-address* **identifier** *identifier-number*
8. **sccp**
9. **sccp ccm group** *group-number*
10. **bind interface** *interface-type interface-number*
11. **associate ccm** *identifier-number* **priority** *priority-number*
12. **associate profile** *profile identifier* **register** *device-name*
13. **keepalive retries** *number*
14. **switchover method** [**graceful** | **immediate**]
15. **switch back method** {**graceful** | **guard** *timeout-guard-value* | **immediate** | **uptime** *uptime-timeout-value*}
16. **switchback interval** *seconds*
17. **exit**
18. **dspfarm profile** *profile-identifier* **transcode** [**security**]
19. **trustpoint** *trustpoint-label*
20. **codec** *codec-type*
21. **maximum sessions** *number*
22. **associate application sccp**
23. **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.

	Command or Action	Purpose
Step 3	**voice-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode for the network module on which you want to enable DSP-farm services.
Step 4	**dsp services dspfarm** **Example:** `Router(config-voicecard)# dsp services dspfarm`	Enables DSP-farm services for the voice card.
Step 5	**exit** **Example:** `Router(config-voicecard)# exit`	Exits voice-card configuration mode.
Step 6	**sccp local** *interface-type interface-number* **Example:** `Router(config)# sccp local FastEthernet 0/0`	Selects the local interface that the SCCP applications (transcoding and conferencing) should use to register with Cisco Unified CME. • *interface-type*—Interface type that the SCCP application uses to register with Cisco Unified CME. The type can be an interface address or a virtual-interface address such as Ethernet. • *interface-number*—Interface number that the SCCP application uses to register with Cisco Unified CME.
Step 7	**sccp ccm** *ip-address* **identifier** *identifier-number* **Example:** `Router(config)# sccp ccm 10.10.10.1 identifier 1`	Specifies the Cisco Unified CME address. • *ip-address*—IP address of the Cisco Unified CME router. • **identifier** *identifier-number*—Number that identifies the Cisco Unified CME router. • Repeat this step to specify the address of a secondary Cisco Unified CME router.
Step 8	**sccp** **Example:** `Router(config)# sccp`	Enables SCCP and its associated transcoding and conferencing applications.
Step 9	**sccp ccm group** *group-number* **Example:** `Router(config)# sccp ccm group 1`	Creates a Cisco Unified CME group and enters SCCP configuration mode for Cisco Unified CME. • *group-number*—Number that identifies the Cisco Unified CME group. **Note** A Cisco Unified CME group is a naming device under which data for the DSP farms is declared. Only one group is required.

	Command or Action	Purpose
Step 10	**bind interface** *interface-type interface-number* **Example:** `Router(config-sccp-ccm)# bind interface FastEthernet 0/0`	(Optional) Binds an interface to a Cisco Unified CME group so that the selected interface is used for all calls that belong to the profiles that are associated to this Cisco Unified CME group. • This command is optional, but we recommend it if you have more than one profile or if you are on different subnets, to ensure that the correct interface is selected.
Step 11	**associate ccm** *identifier-number* **priority** *priority-number* **Example:** `Router(config-sccp-ccm)# associate ccm 1 priority 1`	Associates a Cisco Unified CME router with a group and establishes its priority within the group. • *identifier-number*—Number that identifies the Cisco Unified CME router. See the **sccp ccm** command in Step 7, on page 482. • **priority**—The priority of the Cisco Unified CME router in the Cisco Unified CME group. Only one Cisco Unified CME group is possible. Default: 1.
Step 12	**associate profile** *profile identifier* **register** *device-name* **Example:** `Router(config-sccp-ccm)# associate profile 1 register mtp000a8eaca80`	Associates a DSP farm profile with a Cisco Unified CME group. • *profile-identifier*—Number that identifies the DSP farm profile. • *device-name*—MAC address with the "mtp" prefix added, where the MAC address is the burnt-in address of the physical interface that is used to register as the SCCP device.
Step 13	**keepalive retries** *number* **Example:** `Router(config-sccp-ccm)# keepalive retries 5`	Sets the number of keepalive retries from SCCP to Cisco Unified CME. • *number*—Number of keepalive attempts. Range: 1 to 32. Default: 3.
Step 14	**switchover method** [**graceful** | **immediate**] **Example:** `Router(config-sccp-ccm)# switchover method immediate`	Sets the switchover method that the SCCP client uses when its communication link to the active Cisco Unified CME system goes down. • **graceful**—Switchover happens only after all the active sessions have been terminated gracefully. • **immediate**—Switches over to any one of the secondary Cisco Unified CME systems immediately.
Step 15	**switch back method** {**graceful** | **guard** *timeout-guard-value* | **immediate** | **uptime** *uptime-timeout-value*} **Example:** `Router(config-sccp-ccm)# switchback method immediate`	Sets the switch back method that the SCCP client uses when the primary or higher priority Cisco Unified CME becomes available again. • **graceful**—Switchback happens only after all the active sessions have been terminated gracefully.

	Command or Action	Purpose
		• **guard** *timeout-guard-value*—Switchback happens either when the active sessions have been terminated gracefully or when the guard timer expires, whichever happens first. Timeout value is in seconds. Range: 60 to 172800. Default: 7200. • **immediate**—Switches back to the higher order Cisco Unified CME immediately when the timer expires, whether there is an active connection or not. • **uptime** *uptime-timeout-value*—Initiates the uptime timer when the higher-order Cisco Unified CME system comes alive. Timeout value is in seconds. Range: 60 to 172800. Default: 7200.
Step 16	**switchback interval** *seconds* **Example:** `Router(config-sccp-ccm)# switchback interval 5`	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CME system when the current Cisco Unified CME switchback connection fails. • *seconds*—Timer value, in seconds. Range: 1 to 3600. Default: 60.
Step 17	**exit** **Example:** `Router(config-sccp-ccm)# exit`	Exits SCCP configuration mode.
Step 18	**dspfarm profile** *profile-identifier* **transcode** [**security**] **Example:** `Router(config)# dspfarm profile 1 transcode security`	Enters DSP farm profile configuration mode and defines a profile for DSP farm services. • *profile-identifier*—Number that uniquely identifies a profile. Range: 1 to 65535. • **transcode**—Enables profile for transcoding. • **security**—Enables secure DSP farm services. This keyword is supported in Cisco Unified CME 4.2 and later versions.
Step 19	**trustpoint** *trustpoint-label* **Example:** `Router(config-dspfarm-profile)# trustpoint dspfarm`	(Optional) Associates a trustpoint with a DSP farm profile.
Step 20	**codec** *codec-type* **Example:** `Router(config-dspfarm-profile)# codec g711ulaw`	Specifies the codecs supported by a DSP farm profile. • *codec-type*—Specifies the preferred codec. Type **?** for a list of supported codecs. • Repeat this step for each supported codec.

	Command or Action	Purpose
Step 21	**maximum sessions** *number* **Example:** `Router(config-dspfarm-profile)# maximum sessions 5`	Specifies the maximum number of sessions that are supported by the profile. • *number*—Number of sessions supported by the profile. Range: 0 to X. Default: 0. • The X value is determined at run time depending on the number of resources available with the resource provider.
Step 22	**associate application sccp** **Example:** `Router(config-dspfarm-profile)# associate application sccp`	Associates SCCP with the DSP farm profile.
Step 23	**end** **Example:** `Router(config-dspfarm-profile)# end`	Returns to privileged EXEC mode.

What to Do Next

- To register the DSP Farm to Cisco Unified CME in secure mode, see Register the DSP Farm with Cisco Unified CME 4.2 or a Later Version in Secure Mode, on page 496.

Configure DSP Farms for NM-HDVs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dsp services dspfarm**
5. **exit**
6. **sccp local** *interface-type interface-number*
7. **sccp ccm** *ip-address* **priority** *priority-number*
8. **sccp**
9. **dsp farm transcoder maximum sessions** *number*
10. **dspfarm**
11. **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-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode and identifies the slot in the chassis in which the NM-HDV or NM-HDV farm is located.
Step 4	**dsp services dspfarm** **Example:** `Router(config-voicecard)# dsp services dspfarm`	Enables DSP-farm services on the NM-HDV or NM-HDV farm.
Step 5	**exit** **Example:** `Router(config-voicecard)# exit`	Returns to global configuration mode.
Step 6	**sccp local** *interface-type interface-number* **Example:** `Router(config)# sccp local FastEthernet 0/0`	Selects the local interface that the SCCP applications (transcoding and conferencing) should use to register with Cisco Unified CME. • *interface-type*—Interface type that the SCCP application uses to register with Cisco Unified CME. The type can be an interface address or a virtual-interface address such as Ethernet. • *interface-number*—Interface number that the SCCP application uses to register with Cisco Unified CME.
Step 7	**sccp ccm** *ip-address* **priority** *priority-number* **Example:** `Router(config)# sccp ccm 10.10.10.1 priority 1`	Specifies the Cisco Unified CME address. • *ip-address*—IP address of the Cisco Unified CME router. • **priority** *priority*—Priority of the Cisco Unified CME router relative to other connected routers. Range: 1 (highest) to 4 (lowest).
Step 8	**sccp** **Example:** `Router(config)# sccp`	Enables SCCP and its associated transcoding and conferencing applications.

	Command or Action	Purpose
Step 9	**dsp farm transcoder maximum sessions** *number* **Example:** `Router(config)# dspfarm transcoder maximum sessions 12`	Specifies the maximum number of transcoding sessions to be supported by the DSP farm. A DSP can support up to four transcoding sessions. **Note** When you assign this value, take into account the number of DSPs allocated for conferencing services.
Step 10	**dspfarm** **Example:** `Router(config)# dspfarm`	Enables the DSP farm.
Step 11	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configure the Cisco Unified CME Router to Act as the DSP Farm Host

Determine the Maximum Number of Transcoder Sessions

To determine the maximum number of transcoder sessions that can occur at one time perform the following steps.

Step 1 Use the **dspfarm transcoder maximum sessions** command to set the maximum number of transcoder sessions you have configured.

Step 2 Use the **show sdspfarm sessions** command to display the number of transcoder sessions that are active.

Step 3 Use the **show sdspfarm units** command to display the number of DSP farms that are configured.

Step 4 Obtain the maximum number of transcoder sessions by multiplying the number of transcoder sessions from Step 2 (configured in Step 1 using the **dspfarm transcoder maximum sessions** command) by the number of DSP farms from Step 3.

Set the Cisco Unified CME Router to Receive IP Phone Messages

Note You can unregister all active calls' transcoding streams with the **sdspfarm unregister force** command.

Before You Begin

Identify the MAC address of the SCCP client interface. For example, if you have the following configuration:

```
interface FastEthernet 0/0
 ip address 10.5.49.160 255.255.0.0
 .
 .
 .
sccp local FastEthernet 0/0
 sccp
```

The **show interface FastEthernet 0/0** command will yield a MAC address. In the following example, the MAC address of the Fast Ethernet interface is 000a.8aea.ca80:

```
Router# show interface FastEthernet 0/0
.
.
.
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000a.8aea.ca80 (bia 000a.8aea.ca80)
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**]
5. **sdspfarm units** *number*
6. **sdspfarm transcode sessions** *number*
7. **sdspfarm tag** *number device-name*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**]	Enables a router to receive messages from Cisco Unified IP phones through the router's IP addresses and ports.

	Command or Action	Purpose
	Example: `Router(config-telephony)# ip source address 10.10.10.1 port 3000`	• *address*—Range: 0 to 5. Default: 0. • **port** *port*—(Optional) TCP/IP port used for SCCP. Default: 2000. • **any-match**—(Optional) Disables strict IP address checking for registration. This is the default. • **strict-match**—(Optional) Requires strict IP address checking for registration.
Step 5	**sdspfarm units** *number* **Example:** `Router(config-telephony)# sdspfarm units 4`	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP router. • *number*—Range: 0 to 5. Default: 0.
Step 6	**sdspfarm transcode sessions** *number* **Example:** `Router(config-telephony)# sdspfarm transcode sessions 40`	Specifies the maximum number of transcoder sessions for G.729 allowed by the Cisco Unified CME router. • One transcoder session consists of two transcoding streams between callers using transcode. Use the maximum number of transcoding sessions and conference calls that you want your router to support at one time. • *number*—See Determine the Maximum Number of Transcoder Sessions, on page 487. Range: 0 to 128. Default: 0.

Step 7	**sdspfarm tag** *number device-name*
	
	Example:
	`Router(config-telephony)# sdspfarm tag 1 mtp000a8eaca80`
	or
	`Router(config-telephony)# sdspfarm tag 1 MTP000a8eaca80`
		Permits a DSP farm unit to be registered to Cisco Unified CME and associates it with an SCCP client interface's MAC address.
		• Required only if you blocked automatic registration by using the **auto-reg-ephone** command.
		• *number*—The tag number. Range: 1 to 5.
		• *device-name*—MAC address of the SCCP client interface with the "MTP" prefix added.

Step 8	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure the Cisco Unified CME Router to Host a Secure DSP Farm

You must configure the Media Encryption Secure Real-Time Transport Protocol (SRTP) feature in the Cisco Unified CME 4.2 and later versions, making it a secure Cisco Unified CME, before it can host a secure

DSP farm. For information on configuring a secure Cisco Unified CME, see Configure Security, on page 597.

Modify DSP Farms for NM-HDVs After Upgrading Cisco IOS Software

To ensure continued support for existing DSP farms for NM-HDVs configured after upgrading the Cisco IOS software on your Cisco router, perform the following steps.

Note Perform this task if previously-configured DSP farms for NM-HDVs fail to register to Cisco Unified CME after you upgrade the Cisco IOS software release.

Before You Begin

Confirm that device name for a dspfarm tag in telephony-service configuration is lower case by using the **show-running configuration** command.

```
Example:

Router#show-running configuration
Building configuration...
.
.
.
!
telephony-service
 max-ephones 2
 max-dn 20
 ip source-address 142.103.66.254 port 2000
 auto assign 1 to 2
 system message Your current options
 sdspfarm units 2
 sdspfarm transcode sessions 16
 sdspfarm tag 1 mtp00164767cc20   !<===Device name is MAC address with lower-case “mtp” prefix
.
.
.
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no sdspfarm tag** *number*
4. **sdspfarm tag** *number device-name*
5. **dspfarm**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no sdspfarm tag** *number* **Example:** `Router(config)# no sdspfarm tag 1`	Disables the DSP farm.
Step 4	**sdspfarm tag** *number device-name* **Example:** `Router(config)# sdspfarm tag 1 MTP00164767cc20`	Permits a digital-signal-processor (DSP) farm to be to registered to Cisco Unified CME and associates it with a SCCP client interface's MAC address. • Required only if you blocked automatic registration by using the **auto-reg-ephone** command. • *device-name*—MAC address of the SCCP client interface with the "MTP" prefix added.
Step 5	**dspfarm** **Example:** `Router(config)# dspfarm`	Enables the DSP farm.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Modify the Number of Transcoding Sessions for NM-HDVs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no dspfarm**
4. **dspfarm transcoder maximum sessions** *number*
5. **dspfarm**
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	**no dspfarm** **Example:** `Router(config)# no dspfarm`	Disables the DSP farm.
Step 4	**dspfarm transcoder maximum sessions** *number* **Example:** `Router(config)# dspfarm transcoder maximum sessions 12`	Specifies the maximum number of transcoding sessions to be supported by the DSP farm.
Step 5	**dspfarm** **Example:** `Router(config)# dspfarm`	Enables the DSP farm.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Tune DSP-Farm Performance on an NM-HDV

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp ip precedence** *value*
4. **dspfarm rtp timeout** *seconds*
5. **dspfarm connection interval** *seconds*
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	**sccp ip precedence** *value* **Example:** `Router(config)# sccp ip precedence 5`	(Optional) Sets the IP precedence value to increase the priority of voice packets over connections controlled by SCCP.
Step 4	**dspfarm rtp timeout** *seconds* **Example:** `Router(config)# dspfarm rtp timeout 60`	(Optional) Configures the Real-Time Transport Protocol (RTP) timeout interval if the error condition "RTP port unreachable" occurs.
Step 5	**dspfarm connection interval** *seconds* **Example:** `Router(config)# dspfarm connection interval 60`	(Optional) Specifies how long to monitor RTP inactivity before deleting an RTP stream.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Verify DSP Farm Operation

To verify that the DSP farm is registered and running, perform the following steps in any order.

Step 1 Use the **show sccp** [**statistics** | **connections**] command to display the SCCP configuration information and current status.

Example:

```
Router# show sccp statistics
SCCP Application Service(s) Statistics:

Profile ID:1, Service Type:Transcoding
TCP packets rx 7, tx 7
Unsupported pkts rx 1, Unrecognized pkts rx 0
```

```
Register tx 1, successful 1, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
Reset rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

Use the **show sccp connections** command to display information about the connections controlled by the SCCP transcoding and conferencing applications. In the following example, the secure value of the stype field indicates that the connection is encrypted:

```
Router# show sccp connections

sess_id    conn_id     stype            mode     codec  ripaddr      rport sport

16777222   16777409   secure-xcode sendrecv g729b 10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u 10.3.56.50    17030 18464
Total number of active session(s) 1, and connection(s) 2
```

Step 2 Use the **show sdspfarm units** command to display the configured and registered DSP farms.

Example:

```
Router# show sdspfarm units

mtp-1 Device:MTP003080218a31 TCP socket:[2]  REGISTERED
actual_stream:8 max_stream 8 IP:10.10.10.3  11470  MTP YOKO keepalive 1
Supported codec:G711Ulaw
                 G711Alaw
                 G729a
                 G729ab

 max-mtps:1, max-streams:40, alloc-streams:8, act-streams:2
```

Step 3 Use the **show sdspfarm sessions** command to display the transcoding streams.

Example:

```
Router# show sdspfarm sessions
Stream-ID:1 mtp:1 10.10.10.3  18404  Local:2000 START
 usage:Ip-Ip
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:2

Stream-ID:2 mtp:1 10.10.10.3  17502  Local:2000 START
 usage:Ip-Ip
 codec:G729AnnexA  duration:20 vad:0 peer Stream-ID:1

Stream-ID:3 mtp:1 0.0.0.0  0  Local:0 IDLE
 usage:
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0

Stream-ID:4 mtp:1 0.0.0.0  0  Local:0 IDLE
 usage:
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0

Stream-ID:5 mtp:1 0.0.0.0  0  Local:0 IDLE
 usage:
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0

Stream-ID:6 mtp:1 0.0.0.0  0  Local:0 IDLE
 usage:
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0

Stream-ID:7 mtp:1 0.0.0.0  0  Local:0 IDLE
 usage:
```

```
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0

Stream-ID:8 mtp:1 0.0.0.0  0  Local:0 IDLE
 usage:
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
```

Step 4 Use the **show sdspfarm sessions summary** command to display a summary view the transcoding streams.

Example:

```
Router# show sdspfarm sessions summary

max-mtps:2, max-streams:240, alloc-streams:40, act-streams:2
  ID   MTP  State      CallID confID Usage                         Codec/Duration
==== ===== ====== =========== ====== ============================= ==============
1    2     IDLE   -1          0                                   G711Ulaw64k /20ms
2    2     IDLE   -1          0                                   G711Ulaw64k /20ms
3    2     START  -1          3      MoH  (DN=3  , CH=1) FE=TRUE  G729 /20ms
4    2     START  -1          3      MoH  (DN=3  , CH=1) FE=FALSE G711Ulaw64k /20ms
5    2     IDLE   -1          0                                   G711Ulaw64k /20ms
6    2     IDLE   -1          0                                   G711Ulaw64k /20ms
7    2     IDLE   -1          0                                   G711Ulaw64k /20ms
8    2     IDLE   -1          0                                   G711Ulaw64k /20ms
9    2     IDLE   -1          0                                   G711Ulaw64k /20ms
10   2     IDLE   -1          0                                   G711Ulaw64k /20ms
11   2     IDLE   -1          0                                   G711Ulaw64k /20ms
12   2     IDLE   -1          0                                   G711Ulaw64k /20ms
13   2     IDLE   -1          0                                   G711Ulaw64k /20ms
14   2     IDLE   -1          0                                   G711Ulaw64k /20ms
15   2     IDLE   -1          0                                   G711Ulaw64k /20ms
16   2     IDLE   -1          0                                   G711Ulaw64k /20ms
17   2     IDLE   -1          0                                   G711Ulaw64k /20ms
18   2     IDLE   -1          0                                   G711Ulaw64k /20ms
19   2     IDLE   -1          0                                   G711Ulaw64k /20ms
20   2     IDLE   -1          0                                   G711Ulaw64k /20ms
21   2     IDLE   -1          0                                   G711Ulaw64k /20ms
22   2     IDLE   -1          0                                   G711Ulaw64k /20ms
23   2     IDLE   -1          0                                   G711Ulaw64k /20ms
24   2     IDLE   -1          0                                   G711Ulaw64k /20ms
25   2     IDLE   -1          0                                   G711Ulaw64k /20ms
26   2     IDLE   -1          0                                   G711Ulaw64k /20ms
27   2     IDLE   -1          0                                   G711Ulaw64k /20ms
28   2     IDLE   -1          0                                   G711Ulaw64k /20ms
29   2     IDLE   -1          0                                   G711Ulaw64k /20ms
30   2     IDLE   -1          0                                   G711Ulaw64k /20ms
31   2     IDLE   -1          0                                   G711Ulaw64k /20ms
32   2     IDLE   -1          0                                   G711Ulaw64k /20ms
33   2     IDLE   -1          0                                   G711Ulaw64k /20ms
34   2     IDLE   -1          0                                   G711Ulaw64k /20ms
35   2     IDLE   -1          0                                   G711Ulaw64k /20ms
36   2     IDLE   -1          0                                   G711Ulaw64k /20ms
```

Step 5 Use the **show sdspfarm sessions active** command to display the transcoding streams for all active sessions.

Example:

```
Router# show sdspfarm sessions active

Stream-ID:1 mtp:1 10.10.10.3  18404  Local:2000 START
 usage:Ip-Ip
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:2

Stream-ID:2 mtp:1 10.10.10.3  17502  Local:2000 START
 usage:Ip-Ip
 codec:G729AnnexA  duration:20 vad:0 peer Stream-ID:1
```

Step 6 Use the **show sccp connections details** command to display the SCCP connections details such as call-leg details.

Example:

```
Router# show sccp connections details

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id    codec   pkt-period type      bridge-info(bid, cid)
mmbridge-info(bid, cid)

1          -          14         N/A     N/A        transmsp  All RTPSPI Callegs      N/A


1          2          15         g729a   20         rtpspi    (4,14)                  N/A


1          1          13         g711u   20         rtpspi    (3,14)                  N/A


Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Step 7 Use the **debug sccp** {**all** | **errors** | **events** | **packets** | **parser**} command to set debugging levels for SCCP and its applications.

Step 8 Use the **debug dspfarm** {**all** | **errors** | **events** | **packets**} command to set debugging levels for DSP-farm service.

Step 9 Use the **debug ephone mtp** command to enable Message Transfer Part (MTP) debugging. Use this debug command with the **debug ephone mtp**, **debug ephone register**, **debug ephone state**, and **debug ephone pak** commands.

Register the DSP Farm with Cisco Unified CME 4.2 or a Later Version in Secure Mode

The DSP farm can reside on the same router with the Cisco Unified CME or on a different router. Some of the steps in the following tasks are optional depending the location of the DSP farm.

Obtain Digital Certificate from a CA Server

The CA server can be the same router as the DSP farm. The DSP farm router can be configured as a CA server. The configuration steps below show how to configure a CA server on the DSP farm router. Additional configurations are required for configuring CA server on an external Cisco router or using a different CA server by itself.

Configure a CA Server

Note Skip this procedure if the DSP farm resides on the same router as the Cisco Unified CME. Proceed to the Create a Trustpoint, on page 499 section.

The CA server automatically creates a trustpoint where the certificates are stored. The automatically created trustpoint stores the CA root certificate.

Before You Begin

- Cisco Unified CME 4.2 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki server** *label*
4. **database level complete**
5. **grant auto**
6. **database url** *root-url*
7. **no shutdown**
8. **exit**
9. **crypto pki trustpoint** *label*
10. **revocation-check crl**
11. **rsakeypair** *key-label*

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	**crypto pki server** *label* **Example:** `Router(config)# crypto pki server dspcert`	Defines a label for the certificate server and enters certificate-server configuration mode. • *label*—Name for CA certificate server.
Step 4	**database level complete** **Example:** `Router(cs-server)# database level complete`	(Optional) Controls the type of data stored in the certificate enrollment database. The default if this command is not used is **minimal**. • **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; so specify an external TFTP server in which to store the data using of the **database url** command.

	Command or Action	Purpose
Step 5	**grant auto** **Example:** `Router(cs-server)# grant auto`	(Optional) Allows an automatic certificate to be issued to any requester. The recommended method and default if this command is not used is manual enrollment. **Tip** Use this command only during enrollment when testing and building simple networks. A security best practice is to disable this functionality using the **no grant auto** command after configuration so that certificates cannot be continually granted.
Step 6	**database url** *root-url* **Example:** `Router(cs-server)# database url nvram:`	(Optional) Specifies the location where all database entries for the certificate server are to be written out. If this command is not specified, all database entries are written to NVRAM. • *root-url*—Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system. **Note** If the CA is going to issue a large number of certificates, select an appropriate storage location like flash or other storage device to store the certificates. **Note** When the storage location chosen is flash and the file system type on this device is Class B (LEFS), make sure to check free space on the device periodically and use the **squeeze** command to free the space used up by deleted files. This process may take several minutes and should be done during scheduled maintenance periods or off-peak hours.
Step 7	**no shutdown** **Example:** `Router(cs-server)# no shutdown`	(Optional) Enables the CA. **Note** You should use this command only after you have completely configured the CA.
Step 8	**exit** **Example:** `Router(cs-server)# exit`	Exits certificate-server configuration mode.
Step 9	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint dspcert`	(Optional) Declares a trustpoint and enters ca-trustpoint configuration mode. • *label*—Name for the trustpoint. **Note** Use this command and the **enrollment url** command if this CA is local to the Cisco Unified CME router. These commands are not needed for a CA running on an external router. The *label* has to be the same as the *label* in Step 3.
Step 10	**revocation-check crl** **Example:** `Router(ca-trustpoint)# revocation-check crl`	(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down. • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior.

	Command or Action	Purpose
Step 11	**rsakeypair** *key-label* **Example:** `Router(ca-trustpoint)# rsakeypair caserver`	(Optional) Specifies an RSA key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is used. **Note** Multiple trustpoints can share the same key.

Create a Trustpoint

The trustpoint stores the digital certificate for the DSP farm. To create a trustpoint, perform the following procedure:

Before You Begin

- Cisco Unified CME 4.2 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **serial-number none**
6. **fqdn none**
7. **ip-address none**
8. **subject-name** [*x.500-name*]
9. **revocation-check none**
10. **rsakeypair** *key-label*

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.

	Command or Action	Purpose
Step 3	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint dspcert`	Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode. • *label*—Name for the trustpoint and RA.
Step 4	**enrollment url** *ca-url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.3.105.40:80`	Specifies the enrollment URL of the issuing CA certificate server (root certificate server). • *ca-url*—URL of the router on which the root CA is installed.
Step 5	**serial-number none** **Example:** `Router(ca-trustpoint)# serial-number none`	Specifies whether the router serial number should be included in the certificate request. • **none**—Specifies that a serial number will not be included in the certificate request.
Step 6	**fqdn none** **Example:** `Router(ca-trustpoint)# fqdn none`	Specifies a fully qualified domain name (FQDN) that will be included as "unstructuredName" in the certificate request. • **none**—Router FQDN will not be included in the certificate request.
Step 7	**ip-address none** **Example:** `Router(ca-trustpoint)# ip-address none`	Specifies a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request.
Step 8	**subject-name** [*x.500-name*] **Example:** `Router(ca-trustpoint)# subject-name cn=vg224, ou=ABU, o=Cisco Systems Inc.`	Specifies the subject name in the certificate request. **Note** The example shows how to format the certificate subject name to be similar to that of an IP phones.
Step 9	**revocation-check none** **Example:** `Router(ca-trustpoint)# revocation-check none`	(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down. • **none**—Certificate checking is not required.
Step 10	**rsakeypair** *key-label* **Example:** `Router(ca-trustpoint)# rsakeypair dspcert`	(Optional) Specifies an RSA key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is used. **Note** Multiple trustpoints can share the same key. The *key-label* is the same as the *label* in Step 3.

	Command or Action	Purpose

Authenticate and Enroll a Certificate with the CA Server

Before You Begin

- Cisco Unified CME 4.2 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki authenticate** *trustpoint-label*
4. **crypto pki enroll** *trustpoint-label*

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	**crypto pki authenticate** *trustpoint-label* **Example:** `Router(config)# crypto pki authenticate dspcert`	Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint if prompted. • *trustpoint-label*—Trustpoint label. **Note** The *trustpoint-label* is the trustpoint label specified in the Create a Trustpoint, on page 499 section.
Step 4	**crypto pki enroll** *trustpoint-label* **Example:** `Router(config)# crypto pki enroll dspcert`	Enrolls with the CA and obtains the certificate for this trustpoint. • *trustpoint-label*—Trustpoint label. **Note** The *trustpoint-label* is the trustpoint label specified in the Create a Trustpoint, on page 499 section.

Copy the CA Root Certificate of the DSP Farm Router to the Cisco Unified CME Router

The DSP farm router and Cisco Unified CME router exchanges certificates during the registration process. These certificates are digitally signed by the CA server of the respective router. For the routers to accept each others digital certificate, they should have the CA root certificate of each other. Manually copy the CA root certificate of the DSP farm and Cisco Unified CME router to each other.

Before You Begin

- Cisco Unified CME 4.2 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment terminal**
5. **crypto pki export** *trustpoint* **pem terminal**
6. **crypto pki authenticate** *trustpoint-label*
7. You will be prompted to enter the CA certificate. Cut and paste the base 64 encoded certificate at the command line, then press Enter, and type "quit". The router prompts you to accept the certificate. Enter "yes" to accept the certificate.

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	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint dspcert`	Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode. • *label*—Name for the trustpoint and RA. **Note** The *label* is the trustpoint label specified in the Create a Trustpoint, on page 499 section.
Step 4	**enrollment terminal** **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment.

	Command or Action	Purpose
Step 5	**crypto pki export** *trustpoint* **pem terminal** **Example:** `Router(ca-trustpoint)# crypto pki export dspcert pem terminal`	Exports certificates and RSA keys that are associated with a trustpoint in a privacy-enhanced mail (PEM)-formatted file.
Step 6	**crypto pki authenticate** *trustpoint-label* **Example:** `Router(config)# crypto pki authenticate vg224`	Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint if prompted. • *trustpoint-label*—Trustpoint label. **Note** This command is optional if the CA certificate is already loaded into the configuration.
Step 7	You will be prompted to enter the CA certificate. Cut and paste the base 64 encoded certificate at the command line, then press Enter, and type "quit". The router prompts you to accept the certificate. Enter "yes" to accept the certificate.	Completes the copying of the CA root certificate of the DSP farm router to the Cisco Unified CME router.

Copy CA Root Certificate of the Cisco Unified CME Router to the DSP Farm Router

Repeat the steps in the Copy the CA Root Certificate of the DSP Farm Router to the Cisco Unified CME Router, on page 502 section in the opposite direction, that is, from Cisco Unified CME router to the DSP farm router.

Prerequisites

- Cisco Unified CME 4.2 or a later version.

Configure Cisco Unified CME to Allow the DSP Farm to Register

Before You Begin

- Cisco Unified CME 4.2 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **sdspfarm units** *number*
5. **sdspfarm transcode sessions** *number*
6. **sdspfarm tag** *number device-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**sdspfarm units** *number* **Example:** `Router(config-telephony)# sdspfarm units 1`	Specifies the maximum number of digital-signal-processor (DSP) farms that are allowed to be registered to the Skinny Client Control Protocol (SCCP) server.
Step 5	**sdspfarm transcode sessions** *number* **Example:** `Router(config-telephony)# sdspfarm transcode sessions 30`	Specifies the maximum number of transcoding sessions allowed per Cisco Unified CME router. • *number*—Declares the number of DSP farm sessions. Valid values are numbers from 1 to 128.
Step 6	**sdspfarm tag** *number device-name* **Example:** `Router(config-telephony)# sdspfarm tag 1 vg224`	Permits a DSP farm to register to Cisco Unified CME and associates it with a SCCP client interfaces MAC address. **Note** The *device-name* in this step must be the same as the *device-name* in the **associate profile** command in Step 17 of the Configure DSP Farms for NM-HDs and NM-HDV2s, on page 481 section.
Step 7	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.

Verify DSP Farm Registration with Cisco Unified CME

Use the **show sdspfarm units** command to verify that the DSP farm is registering with Cisco Unified CME. Use the **show voice dsp group slot** command to show the status of secure conferencing.

Prerequisites

- Cisco Unified CME 4.2 or a later version.

show sdspfarm units

```
Router# show sdspfarm units

mtp-2 Device:choc2851SecCFB1 TCP socket:[1]  REGISTERED
actual_stream:8 max_stream 8 IP:10.1.0.20  37043  MTP YOKO keepalive 17391
Supported codec: G711Ulaw
                 G711Alaw
                 G729
                 G729a
                 G729ab
                 GSM FR

 max-mtps:2, max-streams:60, alloc-streams:18, act-streams:0
```

show voice dsp

```
Router# show voice dsp group slot 1

dsp 13:
  State: UP, firmware: 4.4.706
  Max signal/voice channel: 16/16
  Max credits: 240
  Group: FLEX_GROUP_VOICE, complexity: FLEX
    Shared credits: 180, reserved credits: 0
    Signaling channels allocated: 2
    Voice channels allocated: 0
    Credits used: 0
  Group: FLEX_GROUP_XCODE, complexity: SECURE MEDIUM
    Shared credits: 0, reserved credits: 60
    Transcoding channels allocated: 0
    Credits used: 0
dsp 14:
  State: UP, firmware: 1.0.6
  Max signal/voice channel: 16/16
  Max credits: 240
  Group: FLEX_GROUP_CONF, complexity: SECURE CONFERENCE
    Shared credits: 0, reserved credits: 240
    Conference session: 1
    Credits used: 0
```

Configure LTI-based Transcoding

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dsp services dspfarm**
5. **exit**
6. **dspfarm profile** *profile-identifier* **transcode** [**universal**]
7. **codec** *codec-type*
8. **maximum sessions** *number*
9. **associate application CUBE**
10. **no shutdown**
11. **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-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode for the network module on which you want to enable DSP-farm services.
Step 4	**dsp services dspfarm** **Example:** `Router(config-voicecard)# dsp services dspfarm`	Enables DSP-farm services for the voice card.
Step 5	**exit** **Example:** `Router(config-voicecard)# exit`	Exits voice-card configuration mode.

	Command or Action	Purpose
Step 6	**dspfarm profile** *profile-identifier* **transcode** [**universal**] **Example:** `Router(config)# dspfarm profile 1 transcode universal`	Enters DSP farm profile configuration mode and defines a profile for DSP farm services. • *profile-identifier*—Number that uniquely identifies a profile. Range: 1 to 65535. • **transcode—**Enables profile for transcoding. • **universal—**Enables transcoding support between all codecs for DSP farm services. Without **universal**, transcoding is always from g711ulaw to any other codec. This keyword is supported in Cisco Unified CME 11.6 and later versions for Cisco 4000 Series ISR.
Step 7	**codec** *codec-type* **Example:** `Router(config-dspfarm-profile)# codec g711ulaw`	Specifies the codecs supported by a DSP farm profile. • *codec-type*—Specifies the preferred codec. Type **?** for a list of supported codecs. • Repeat this step for each supported codec.
Step 8	**maximum sessions** *number* **Example:** `Router(config-dspfarm-profile)# maximum sessions 5`	Specifies the maximum number of sessions that are supported by the profile. • *number*—Number of sessions supported by the profile. If the variable is not configured or if the DSP resources are not available, the value is set to 0. • The X value is determined at run time depending on the number of resources available with the resource provider.
Step 9	**associate application CUBE** **Example:** `Router(config-dspfarm-profile)# associate application CUBE`	Associates CUBE with the DSP farm profile.
Step 10	**no shutdown** **Example:** `Router(config-dspfarm-profile)# no shutdown`	Enables the DSP farm profile.
Step 11	**end** **Example:** `Router(config-dspfarm-profile)# end`	Returns to privileged EXEC mode.

What to Do Next

Note You can use the command **show dspfarm profile** *profile-number* to verify the configured DSP farm profiles. Use the command to verify if the profile status is UP, and the application status is ASSOCIATED.

Configuration Examples for Transcoding Resources

Example for Setting up DSP Farms for NM-HDVs

The following example sets up a DSP farm of 4 DSPs to handle up to 16 sessions (4 sessions per DSP) on a router with an IP address of 10.5.49.160 and a priority of 1 among other servers.

```
voice-card 1
 dsp services dspfarm
 exit
sccp local FastEthernet 0/0
sccp
sccp ccm 10.5.49.160 priority 1
dspfarm transcoder maximum sessions 16
dspfarm

telephony-service
ip source-address 10.5.49.200 port 2000
sdspfarm units 4
sdspfarm transcode sessions  40
sdspfarm tag 1 mtp000a8eaca80
sdspfarm tag 2 mtp123445672012
```

Example for Setting Up DSP Farms for NM-HDs and NM-HDV2s

The following example sets up six transcoding sessions on a router with one DSP farm, an IP address of 10.5.49.160, and a priority of 1 among servers.

```
voice-card 1
 dsp services dspfarm

sccp local FastEthernet 0/1
sccp
sccp ccm 10.5.49.160 identifier 1

sccp ccm group 123
 associate ccm 1 priority
 associate profile 1 register mtp123456792012
 keepalive retries 5
 switchover method immediate
 switchback method immediate
switchback interval 5

dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 maximum sessions 6
 associate application sccp

telephony-service
```

```
 ip source-address 10.5.49.200 port 2000
 sdspfarm units 1
 sdspfarm transcode sessions  40
 sdspfarm tag 1 mtp000a8eaca80
 sdspfarm tag 2 mtp123445672012
```

Example for Configuring Cisco Unified CME Router as the DSP Farm Host

The following example configures Cisco Unified CME router address 10.100.10.11 port 2000 to be the farm host using the DSP farm at mtp000a8eaca80 to allow for a maximum of 1 DSP farm and 16 transcoder sessions.

```
telephony-service
 ip source address 10.100.10.11 port 2000
 sdspfarm units 1
 sdspfarm transcode sessions 16
 sdspfarm tag 1 mtp000a8eaca80
```

Example for Configuring LTI-based Transcoding

The following example configures Cisco Unified CME router for LTI-based transcoding.

```
voice-card 0
 dsp services dspfarm
!--- Dspfarm profile configuration with associate
!--- application CUBE for LTI transcoding.
dspfarm profile 1 transcode universal
codec g729ar8
codec g729br8
codec g711alaw
codec g711ulaw
codec g729r8
maximum sessions 12
associate application CUBE

!--- Only dspfarm profile configurations are needed for
!--- LTI-based transcoding. All the SCCP-based transcoding
!--- features will be supported with LTI-based transcoding.
```

Example for Configuring Voice Class Codec

The following example configures voice class codec under a dial peer on Unified CME.

```
voice class codec 10
 codec preference 1 g711alaw
 codec preference 2 g711ulaw bytes 80
 codec preference 3 g723ar53
 codec preference 4 g723ar63 bytes 144
 codec preference 5 g723r53
 codec preference 6 g723r63 bytes 120
 codec preference 7 g726r16
 codec preference 8 g726r24
 codec preference 9 g726r32 bytes 80
 codec preference 10 g728
 codec preference 11 g729br8
 codec preference 12 g729r8 bytes 50

dial-peer voice 100 voip
 voice-class codec 10
```

You can also configure voice class codec under a voice register pool on Unified CME.

```
voice register pool 1
 id mac 0030.94C2.A22A
 preference 5
 cor incoming call91 1 91011
 translate-outgoing called 1
 proxy 192.0.2.0 preference 1 monitor probe icmp-ping
 alias 1 94... to 91011 preference 8
 voice-class codec 10
```

Where to go Next

Music on Hold

Music on hold can require transcoding resources. See Music on Hold, on page 829.

Teleworker Remote Phones

Transcoding has benefits and disadvantages for remote teleworker phones. See the discussion in Configuring Phones to Make Basic Calls, on page 223.

Feature Information for Transcoding Resources

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

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

Table 34: Feature Information for Transcoding Resources

Feature Name	Cisco Unified CME Version	Feature Information
LTI-based Transcoding	11.6	Support for LTI-based Transcoding on Cisco 4000 Series ISR.
Secure Transcoding	4.2	Secure transcoding for calls using the **codec g729r8 dspfarm-assist** command was introduced.
Transcoding Support	3.2	Transcoding between G.711 and G.729 was introduced.

CHAPTER 14

Toll Fraud Prevention

Prerequisites for Configuring Toll Fraud Prevention

- Cisco Unified CME 8.1 or a later version.
- Cisco IOS Release 15.1(2)T.

Information About Toll Fraud Prevention

Cisco Unified CME 8.1 enhances the Toll Fraud Prevention feature to secure the Cisco Unified CME system against potential toll fraud exploitation by unauthorized users. The following are the enhancements to Toll Fraud Prevention in Cisco Unified CME:

IP Address Trusted Authentication

IP address trusted authentication process blocks unauthorized calls and helps secure the Cisco Unified CME system against potential toll fraud exploitation by unauthorized users. In Cisco Unified CME, **IP address trusted authentication** is enabled by default. When IP address trusted authenticate is enabled, Cisco Unified CME accepts incoming VoIP (SIP/H.323) calls only if the remote IP address of an incoming VoIP call is successfully validated from the system **IP address trusted list**. If the IP address trusted authentication fails, an incoming VoIP call is then disconnected by the application with a user- defined cause code and a new application internal error code 31 message (TOLL_FRAUD_CALL_BLOCK) is logged. For configuration information, see Configure IP Address Trusted Authentication for Incoming VoIP Calls, on page 513.

Cisco Unified CME maintains an **IP address trusted list** to validate the remote IP addresses of incoming VOIP calls. Cisco Unified CME saves an IPv4 session target of VoIP dial-peer to add the trusted IP addresses to **IP address trusted list** automatically.The IPv4 session target is identified as a trusted IP address only if the status of VoIP dial-peer in operation is "UP". Up to 10050 IPv4 addresses can be defined in the trusted IP address list. No duplicate IP addresses are allowed in the trusted IP address list. You can manually add up to 100 trusted IP addresses for incoming VOIP calls. For more information on manually adding trusted IP addresses, see Add Valid IP Addresses For Incoming VoIP Calls, on page 515.

A call detail record (CDR) history record is generated when the call is blocked as a result of IP address trusted authentication failure. A new voice Internal Error Code (IEC) is saved to the CDR history record. The voice IEC error messages are logged to syslog if "voice iec syslog" option is enabled. The following is an IEC toll fraud call rejected syslog display:

```
*Aug 14 19:54:32.507: %VOICE_IEC-3-GW: Application Framework Core: Internal Error (Toll
fraud call rejected): IEC=1.1.228.3.31.0 on callID 3 GUID=AE5066C5883E11DE8026A96657501A09
```

The **IP address trusted list** authentication must be suspended when Cisco Unified CME is defined with "gateway" and a VoIP dial-peer with "session-target ras" is in operational UP status. The incoming VOIP call routing is then controlled by the gatekeeper. Table 35: Administration and Operation States of IP Address Trusted Authentication, on page 512 shows administration state and operational state in different trigger conditions.

Table 35: Administration and Operation States of IP Address Trusted Authentication

Trigger Condition	Administration State	Operation State
When **ip address trusted authenticate** is enabled.	Down	Down
When "gateway" is defined and a VoIP dial-peer with "ras" as a session target is in "UP" operational state	Up	Down
When **ip address trusted authenticate** is enabled and either "gateway" is not defined or no voip dial-peer with "ras" as session target is in "UP" operational state	Up	Up

Note We recommend enabling SIP authentication before enabling Out-of-dialog REFER (OOD-R) to avoid any potential toll fraud threats.

Direct Inward Dial for Incoming ISDN Calls

In Cisco Unified CME 8.1 and later versions the **direct-inward-dial isdn** feature in enabled to prevent the toll fraud for incoming ISDN calls. The called number of an incoming ISDN enbloc dialing call is used to match the outbound dial-peers even if the **direct-inward-dial** option is disabled from a selected inbound plain old telephone service (POTS) dial-peer. If no outbound dial-peer is selected for the outgoing call set up, the incoming ISDN call is disconnected with cause-code “unassigned-number (1)”. For configuration information, see Configure Direct Inward Dial for Incoming ISDN Calls, on page 517.

Disconnect ISDN Calls With No Matching Dial-peer

Cisco Unified CME 8.1 and later versions disconnect unauthorized ISDN calls when no matching inbound voice dial-peer is selected. Cisco Unified CME and voice gateways use the **dial-peer no-match disconnect-cause** command to disconnect an incoming ISDN call when no inbound dial-peer is selected to avoid default POTS dial-peer behavior including two-stage dialing service to handle the incoming ISDN call.

Block Two-stage Dialing Service on Analog and Digital FXO Ports

Cisco Unified CME 8.1 and later versions block the two-stage dialing service which is initiated when an Analog or Digital FXO port goes offhook and the private line automatic ringdown (PLAR) connection is not setup from the voice-port. As a result, no outbound dial-peer is selected for an incoming analog or digital FXO call and no dialed digits are collected from an FXO call. Cisco Unified CME and voice gateways disconnect the FXO call with cause-code “unassigned-number (1)”. Cisco Unified CME uses the **no secondary dialtone** command by default from FXO voice-port to block the two-stage dialing service on Analog or digital FXO ports. For more information on blocking two-stage dialing service on Analog and Digital FXO port, see Block Secondary Dial tone on Analog and Digital FXO Ports, on page 518.

Configure Toll Fraud Prevention

Configure IP Address Trusted Authentication for Incoming VoIP Calls

Restriction

- IP address trusted authentication is skipped if an incoming SIP call is originated from a SIP phone.
- IP address trusted authentication is skipped if an incoming call is an IPv6 call.
- For an incoming VoIP call, IP trusted authentication must be invoked when the IP address trusted authentication is in “UP” operational state.

Before You Begin

- Cisco Unified CME 8.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. ip address trusted authenticate
5. ip-address trusted call-block cause code
6. **end**
7. **show ip address trusted list**

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 voip configuration mode.
Step 4	ip address trusted authenticate **Example:** `Router(conf-voi-serv)# ip address trusted authenticate`	Enables IP address authentication on incoming H.323 or SIP trunk calls for toll fraud prevention support. IP address trusted list authenticate is enabled by default. Use the "**no ip address trusted list authenticate**" command to disable the IP address trusted list authentication.
Step 5	ip-address trusted call-block cause code **Example:** `Router(conf-voi-serv)#ip address trusted call-block cause` **call-reject**	Issues a cause-code when the incoming call is rejected to the IP address trusted authentication. **Note** If the IP address trusted authentication fails, a call-reject (21) cause-code is issued to disconnect the incoming VoIP call.
Step 6	**end** **Example:** `Router()# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose

Step 7	**show ip address trusted list**
	
	Example:
	`Router# #`**show ip address trusted list**
	`IP Address Trusted Authentication`
	` Administration State: UP`
	` Operation State:      UP`
	
	`IP Address Trusted Call Block Cause:`
	call-reject (21)
		Verifies a list of valid IP addresses for incoming H.323 or SIP trunk calls, Call Block cause for rejected incoming calls.

Router #**show ip address trusted list**

```
IP Address Trusted Authentication
 Administration State: UP
 Operation State:      UP

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

VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1

IP Address Trusted List:
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 172.19.245.0 255.255.255.0''
```

Add Valid IP Addresses For Incoming VoIP Calls

Before You Begin

- Cisco Unified CME 8.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **ip address trusted list**
5. **ipv4** {<*ipv4 address*> [<*network mask*>]}
6. **end**
7. **show ip address trusted list**

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 voip configuration mode.

Step 4	**ip address trusted list**
	
	Example:
	`Router(conf-voi-serv)# ip address trusted list`
	`Router(cfg-iptrust-list)#`
		Enters ip address trusted list mode and allows to manually add additional valid IP addresses.

Step 5	**ipv4** {<*ipv4 address*> [<*network mask*>]}
	
	Example:
	`Router(config)#voice service voip`
	`Router(conf-voi-serv)#ip taddress trusted list`
	`Router(cfg-iptrust-list)#ipv4 172.19.245.1`
	`Router(cfg-iptrust-list)#ipv4 172.19.243.1`
		Allows you to add up to 100 IPv4 addresses in **ip address trusted list**. Duplicate IP addresses are not allowed in the ip address trusted list.
		• (Optional) *network mask*— allows to define a subnet IP address.

Step 6	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.
Step 7	**show ip address trusted list** **Example:** `Router# show shared-line`	Displays a list of valid IP addresses for incoming H.323 or SIP trunk calls.

The following example shows 4 IP addresses configured as trusted IP addresses:

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

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

VoIP Dial-peer IPv4 Session Targets:
 Peer Tag        Oper State      Session Target
 --------        ----------      --------------
 11              DOWN            ipv4:1.3.45.1
 1               UP              ipv4:1.3.45.1

IP Address Trusted List:
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
```

Configure Direct Inward Dial for Incoming ISDN Calls

Before You Begin

- Direct-inward-dial isdn is not supported for incoming ISDN overlap dialing call.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service pots**
4. *direct-inward-dial isdn*
5. **exit**

DETAILED STEPS

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

Step 3	**voice service pots**
	
	Example:
	`Router(config)# voice service pots`
	`Router(conf-voi-serv)#`
		Enters voice service configuration mode with voice telephone-service encapsulation type (pots).

	Command or Action	Purpose
Step 4	*direct-inward-dial isdn* **Example:** `Router(conf-voi-serv)#direct-inward-dial isdn`	Enables direct-inward-dial (DID) for incoming ISDN number. The incoming ISDN (enbloc dialing) call is treated as if the digits were received from the DID trunk. The called number is used to select the outgoing dial peer. No dial tone is presented to the caller.
Step 5	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits voice service pots configuration mode.

```
!
voice service voip
 ip address trusted list
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 supplementary-service media-renegotiate
 sip
 registrar server expires max 120 min 120
!
!
dial-peer voice 1 voip
 destination-pattern 5511...
 session protocol sipv2
 session target ipv4:1.3.45.1
 incoming called-number 5522...
 direct-inward-dial
 dtmf-relay sip-notify
 codec g711ulaw
!
dial-peer voice 100 pots
 destination-pattern 91...
 incoming called-number 2...
 forward-digits 4
!
```

Block Secondary Dial tone on Analog and Digital FXO Ports

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port**
4. *no secondary dialtone*
5. **end**
6. **show run**

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-port** **Example:** `Router(config)#voice-p 2/0/0`	Enters voice-port configuration mode. • Type your Analog or Digital FXO port number.
Step 4	*no secondary dialtone* **Example:** `Router((config-voiceport)# no secondary dialtone`	Blocks the secondary dialtone on Analog and Digital FXO port.
Step 5	**end** **Example:** `Router(conf-voiceport)# exit`	Returns to privileged EXEC mode.
Step 6	**show run** **Example:** `Router# show run | sec voice-port 2/0/0`	Verifies that the secondary dial tone is disabled on the specific voice-port.

```
Router# conf t
Router(config)#voice-p 2/0/0
Router(config-voiceport)# no secondary dialtone
!
end
```

```
Router# show run | sec voice-port 2/0/0
Foreign Exchange Office 2/0/0 Slot is 2, Sub-unit is 0, Port is 0
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 ...
 Secondary dialtone is disabled
```

Troubleshooting Tips for Toll Fraud Prevention

When incoming VOIP call is rejected by IP address trusted authentication, a specific internal error code (IEC) **1.1.228.3.31.0** is saved to the call history record. You can monitor the failed or rejected calls using the IEC support. Follow these steps to monitor any rejected calls:

Step 1 Use the **show voice iec description** command to find the text description of an IEC code.

Example:

```
Router# show voice iec description 1.1.228.3.31.0
    IEC Version: 1
    Entity: 1 (Gateway)
    Category: 228 (User is denied access to this service)
    Subsystem: 3 (Application Framework Core)
    Error: 31 (Toll fraud call rejected)
    Diagnostic Code: 0
```

Step 2 View the IEC statistics information using the **Enable iec statistics** command. The example below shows that 2 calls were rejected due to toll fraud call reject error code.

Example:

```
Router# Enable iec statistics
Router(config)#voice statistics type iec
Router#show voice statistics iec since-reboot
Internal Error Code counters
----------------------------
Counters since reboot:
  SUBSYSTEM Application Framework Core [subsystem code 3]
      [errcode  31] Toll fraud call rejected
```

Step 3 Use the **enable IEC syslog** command to verify the syslog message logged when a call with IEC error is released.

Example:

```
Router# Enable iec syslog
Router (config)#voice iec syslog

Feb 11 01:42:57.371: %VOICE_IEC-3-GW: Application Framework Core:
Internal Error (Toll fraud call rejected): IEC=1.1.228.3.31.0 on
callID 288 GUID=DB3F10AC619711DCA7618593A790099E
```

Step 4 Verify the source address of an incoming VOIP call using the **show call history voice last** command.

Example:

```
Router# show call history voice last 1

GENERIC:
SetupTime=3306550 ms
Index=6
...
InternalErrorCode=1.1.228.3.31.0
...
RemoteMediaIPAddress=1.5.14.13
...
```

Step 5 IEC is saved to VSA of Radius Accounting Stop records. Monitor the rejected calls using the external RADIUS server.

Example:

```
Feb 11 01:44:06.527: RADIUS:   Cisco AVpair       [1] 36
"internal-error-code=1.1.228.3.31.0"
```

Step 6 Retrieve the IEC details from cCallHistoryIec MIB object. More information on IEC is available at: Cisco IOS Voice Troubleshooting and Monitoring Guide

Example:

```
getmany 1.5.14.10 cCallHistoryIec
cCallHistoryIec.6.1 = 1.1.228.3.31.0
>getmany 172.19.156.132 cCallHistory
cCallHistorySetupTime.6 = 815385
cCallHistoryPeerAddress.6 = 1300
cCallHistoryPeerSubAddress.6 =
cCallHistoryPeerId.6 = 8000
cCallHistoryPeerIfIndex.6 = 76
cCallHistoryLogicalIfIndex.6 = 0
cCallHistoryDisconnectCause.6 = 15
cCallHistoryDisconnectText.6 = call rejected (21)
cCallHistoryConnectTime.6 = 0
cCallHistoryDisconnectTime.6 = 815387
cCallHistoryCallOrigin.6 = answer(2)
cCallHistoryChargedUnits.6 = 0
cCallHistoryInfoType.6 = speech(2)
cCallHistoryTransmitPackets.6 = 0
cCallHistoryTransmitBytes.6 = 0
cCallHistoryReceivePackets.6 = 0
cCallHistoryReceiveBytes.6 = 0
cCallHistoryReleaseSrc.6 = internalCallControlApp(7)
cCallHistoryIec.6.1 = 1.1.228.3.31.0

>getone 172.19.156.132 cvVoIPCallHistoryRemMediaIPAddr.6
cvVoIPCallHistoryRemMediaIPAddr.6 = 1.5.14.13
```

Feature Information for Toll Fraud Prevention

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

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

Table 36: Feature Information for Toll Fraud Prevention

Feature Name	Cisco Unified CME Version	Feature Information
Toll Fraud Prevention in Cisco Unified CME	8.1	Introduced support for Toll Fraud Prevention feature.

CHAPTER 15

Graphical User Interface

This chapter describes the Cisco Unified Communications Manager Express (Cisco Unified CME) graphical user interface (GUI) and explains how to set it up accounts for system administrators, customer administrators, and phone users.

Prerequisites for Enabling the GUI

- GUI files must be copied into flash memory on the router. For more information, see Install and Upgrade Cisco Unified CME Software, on page 101.
- To use a phone user account in the Cisco Unified CME GUI to configure speed dials on a phone that is enabled for Extension Mobility, Cisco Unified CME GUI 4.2.1 or a later version must be installed on the Cisco router.

Restrictions for Enabling the GUI

- Unified CME GUI does not support configuration, administration, or customer facing features for SIP Phones.

  Unified CME GUI files are version-specific; GUI files for one version of Unified CME are not compatible with any other version of Unified CME. If you are downgrading or upgrading your Unified CME version, you must downgrade or upgrade your GUI files.
- The user name parameter of any authentication credential must be unique. Do not use the same value for a user name when you configure any two or more authentication credentials in Unified CME, such

as the username for any Unified CME GUI account and the user name in a logout or user profile for Extension Mobility.

- Extension Mobility options in Cisco Unified CME GUI 4.2.1 and later versions cannot be accessed from the System Administrator or Customer Administrator login screens.
- To access the GUI, you must use Microsoft Internet Explorer 5.5 or a later version. Other browsers are not supported.
- If you use an XML configuration file to create a customer administrator login, the XML file can have a maximum size of 4000 bytes.
- The password of the system administrator cannot be changed through the GUI. Only the password of a customer administrator or a phone user can be changed through the GUI.
- If more than 100 phones are configured, choosing to display all phones results in a long delay before results appear.

Information About Enabling the GUI

Cisco Unified CME GUI Support

The Cisco Unified CME GUI provides a web-based interface to manage most system-level and phone-based features. In particular, the GUI facilitates the routine additions and changes associated with employee turnover, allowing these changes to be performed by nontechnical staff. The GUI provides three levels of access to support the following user classes:

- System administrator—Able to configure all system-level and phone-based features. This person is familiar with Cisco IOS software and VoIP network configuration.
- Customer administrator—Able to perform routine phone additions and changes without having access to system-level features. This person does not have to be familiar with Cisco IOS software.
- Phone user—Able to program a small set of features on his or her own phone and search the Cisco Unified CME directory. In Cisco Unified CME GUI 4.2.1 and later versions, phone users can use the GUI to set up personal speed dials for an Extension Mobility phone. The same credential for logging into an Extension Mobility phone can be used to log into the Cisco Unified CME GUI.

The user name parameter of any authentication credential must be unique. Do not use the same value for a user name when you configure any two or more authentication credentials in Cisco Unified CME, such as the username for any Cisco United CME GUI account and the user name in a logout or user profile for Extension Mobility.

The Cisco Unified CME GUI uses HTTP to transfer information from the router to the PC of an administrator or phone user. The router must be configured as an HTTP server, and an initial system administrator username and password must be defined from the router command-line interface (CLI). Additional accounts for customer administrators and phone users can be added from the Cisco Unified CME router using Cisco IOS software commands or from a PC using GUI screens.

Cisco Unified CME provides support for eXtensible Markup Language (XML) cascading style sheets (files with a .css suffix) that can be used to customize the browser GUI display.

AAA Authentication

The GUI supports authentication, authorization, and accounting (AAA) authentication for system administrators through a remote server when this capability is enabled with the **ip http authentication** command. If authentication through the server fails, the local router is searched.

Using the **ip http authentication** command prevents unauthorized users from accessing the Cisco Unified CME router. If this command is not used, the *enable* password for the router is the only requirement to authenticate user access to the GUI. Instead, we recommend you use the local or TACACS authentication options, configured as part of a global AAA framework. By explicitly using the **ip http authentication** command, you designate alternative authentication methods, such as by a local login account or by the method that is specified in the AAA configuration on the Cisco Unified CME router. If you select the AAA authentication method, you must also define an authentication method in your AAA configuration.

For information on configuring AAA authentication, see "Configuring Authentication" chapter of Cisco IOS Security Configuration Guide.

Enable the GUI

Enable the HTTP Server

To enable the HTTP server, and specify the path to files for the GUI and a method of user authentication for security, perform the following steps. The HTTP server on a router is disabled by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http path flash:**
5. **ip http authentication** {**aaa** | **enable** | **local** | **tacacs**}
6. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip http server** **Example:** `Router(config)# ip http server`	Enables the HTTP server on the Cisco Unified CME router.
Step 4	**ip http path flash:** **Example:** Router(config)# ip http path flash:	Sets the location of the HTML files used by the HTTP web server to flash memory on the router.
Step 5	**ip http authentication** {**aaa** | **enable** | **local** | **tacacs**} **Example:** Router(config)# ip http authentication aaa	Specifies the method of authentication for the HTTP server. Default is the **enable** keyword. • **aaa—**Indicates that the authentication method used for the AAA login service should be used for authentication. The AAA login service method is specified by the **aaa authentication login** command. • **enable—**Uses the *enable* password. This is the default if this command is not used. • **local—**Uses login username, password, and privilege level access combination specified in the local system configuration (by the **username** command). • **tacacs—**Uses TACACS (or XTACACS) server.
Step 6	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Enable GUI Access for the System Administrator

To define an initial username and password for a system administrator to access the GUI and enable the GUI to be used to set the time and to add directory listings, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **web admin system name** *username* {**password** *string* | **secret** {**0** | **5**} *string*}
5. **dn-webedit**
6. **time-webedit**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**web admin system name** *username* {**password** *string* | **secret** {**0** | **5**} *string*} **Example:** `Router(config-telephony)# web admin system name pwa3 secret 0 wp78pw`	Defines username and password for a system administrator. • **name** *username*—Unique alphanumeric string to identify a user for this authentication credential only. Default is Admin. • **password** *string*—String to verify system administrator's identity. Default is empty string. • **secret** {**0** | **5**} *string*—Digit specifies state of encryption of the string that follows: ◦ **0**—Password that follows is not encrypted. ◦ **5**—Password that follows is encrypted using Message Digest 5 (MD5). **Note** The **secret 5** keyword pair is used in the output of **show** commands when encrypted passwords are displayed. It indicates that the password that follows is encrypted.

	Command or Action	Purpose
Step 5	**dn-webedit** **Example:** `Router(config-telephony)# dn-webedit`	(Optional) Enables the ability to add directory numbers through the web interface. The **no** form of this command disables the ability to create IP phone extension telephone numbers. That ability could disrupt the network wide management of telephone numbers. If this command is not used, the ability to create directory numbers is disabled by default.
Step 6	**time-webedit** **Example:** `Router(config-telephony)# time-webedit`	(Optional) Enables the ability to set the phone time for the Cisco Unified CME system through the web interface. **Note** We do not recommend this method for setting network time. The router should be set up to automatically synchronize its router clock from a network-based clock source using Network Time Protocol (NTP). In the rare case that a network NTP clock source is not available, use the **time-webedit** command to allow manual setting and resetting of the router clock through the GUI.
Step 7	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Access the Cisco Unified CME GUI

To access the Cisco Unified CME router through the GUI to make configuration changes, perform the following steps.

Note In Cisco Unified CME GUI 4.2.1 and later versions, phone users can use the GUI to set up personal speed dials for an Extension Mobility phone. The same credential for logging on to an Extension Mobility phone can be used to log into the Cisco Unified CME GUI.

Restriction

- The Cisco Unified CME GUI requires Microsoft Internet Explorer 5.5 or a later version. Other browsers are not supported.
- Extension Mobility options in Cisco Unified CME GUI 4.2.1 and later versions cannot be accessed from the System Administrator or Customer Administrator login screens.

Step 1 Go to the following URL:

`http://`*router_ipaddress*`/ccme.html`

where *router_ipaddress* is the IP address of your Cisco Unified CME router. For example, if the IP address of your Cisco Unified CME router is 10.10.10.176, enter the following:

```
http://10.10.10.176/ccme.html
```

Enter your username and password at the login screen.

The Cisco Unified CME system evaluates your privilege level and presents the appropriate window. Note that users with Cisco IOS software privilege level 15 also have system-administrator-level privileges in the Cisco Unified CME GUI after being authenticated locally or remotely through AAA. The **ip http authentication** command that is configured on the Cisco Unified CME router determines where authentication occurs.

Step 2 After you login and are authenticated, the system displays one of the following home pages, based on your user level:

- System administrator home page.
- Customer administrator sees a reduced version of the options available on the system administrator page, according to the XML configuration file that the system administrator created.
- Phone user home page.

After you log in successfully, access online help from the Help menu.

Create a Customized XML File for Customer Administrator GUI

The XML configuration file specifies the parameters and features that are available to customer administrators and the parameters and features that are restricted. The file follows a template named xml.template, which conforms to the Cisco XML Document Type Definition (DTD), as documented in the Cisco IP Phone Services Application Development Notes. This template is one of the first Cisco Unified CME files that is downloaded during installation.

To edit and load the XML configuration file, perform the following steps.

Step 1 Copy the XML template and open it in any text editor (see Example for Configuring XML Configuration File Template, on page 534). Name the file something that is meaningful to you and use “xml” as its suffix. For example, you could name the file "custadm.xml".

Step 2 Edit the XML template. Within the template, each line that starts with a title enclosed in angle brackets describes an XML object and matches an entity name in the Cisco CME GUI. For example, “<AddExtension>” refers to the Add Extension capability, and “<Type>” refers to the Type field on the Add Extension window. For each object in the template, you have a choice of actions. Your choices appear within brackets; for example, “[Hide | Show]” indicates that you have a choice between whether this object is hidden or visible when a customer administrator logs in to the GUI. Delete the action that you do not want and the vertical bar and brackets around the actions.

Example:

For example, to hide the Sequence Number field, change the following text in the template file:

```
<SequenceNumber> [Hide | Show] </SequenceNumber>
```

to the following text in your configuration file:

```
<SequenceNumber> Hide </SequenceNumber>
```

Edit every line in the template until you have changed each choice in brackets to a single action and you have removed the vertical bars and brackets. A sample XML file is shown in the Example for Configuring XML Configuration File, on page 535.

Step 3 Copy the file to a TFTP or FTP server that can be accessed by the Cisco Unified CME router.

Step 4 Copy your file to flash memory on the Cisco Unified CME router.

Example:

```
Router# copy tftp flash
```

Step 5 Load the XML file from router flash memory.

Example:

```
Router(config)# telephony-service
Router(config-telephony)# web customize load filename
Router(config-telephony)# exit
```

GUI Access for Customer Administrators

Prerequisites for Enabling GUI Access to Customer Administrators

- Enable a system administrator account for GUI access. See Enable GUI Access for the System Administrator, on page 526.

- Create the XML configuration file for the customer administrator GUI. See Create a Customized XML File for Customer Administrator GUI, on page 529.
- Reload the XML file using the **web customize load** command if you have made changes to the customer administrator GUI.

Define a Customer Administrator Account Using GUI

Step 1 From the Configure System Parameters menu, choose **Administrator's Login Account**.

Step 2 Complete the **Admin User Name** (username) and **Admin User Type** (Customer) fields. The username must be a unique alphanumeric string to identify a user for this authentication credential only.

Step 3 Complete the **New Password** field for the user that you are defining as a customer administrator. Type the password again to confirm it.

Step 4 Click **Change** for your changes to become effective.

Define a Customer Administrator Account Using Cisco IOS Software Commands

To allow the system administrator to create a customer administrator account by using the Cisco IOS software command line interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **web admin customer name** *username* **password** *string*
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.

	Command or Action	Purpose
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**web admin customer name** *username* **password** *string* **Example:** `Router(config-telephony)# web admin customer name user44 password pw10293847`	Defines a username and password for a customer administrator. • **name** *username*—Unique alphanumeric string to identify a user for this authentication credential only. Default is Customer. • **password** *string*—String to verify customer administrator identity.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

GUI Access for Phone Users

Prerequisites for Enabling GUI Access for Phone Users

- Enable a system administrator account for GUI access. See Enable GUI Access for the System Administrator, on page 526.

Define a Phone User Account Using GUI

To create a phone user account by using the Cisco Unified CME GUI, perform the following steps.

Step 1 From the Configure Phones menu, choose **Add Phone** to add GUI access for a user with a new phone or **Change Phone** to add GUI access for a user with an existing phone. The Add Phone screen or the Change Phone screen appears.

Step 2 Enter a username and password in the **Login Account** area of the screen. The username must be a unique alphanumeric string to identify a user for this authentication credential only. If you are adding a new phone, complete the other fields as appropriate.

Step 3 Click **Change** for your edits to become effective.

Define a Phone User Account Using Cisco IOS Software Commands

To use commands in the ephone configuration mode to create credentials for phone users to log into the Cisco Unified CME GUI, perform the following steps for each phone user/phone combination.

Note You can also create phone user credentials for accessing the Cisco Unified CME GUI by using the **user** command in the voice user-profile configuration mode and the voice logout-profile mode. For configuration information, see Extension Mobility, on page 725.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **username** *username* **password** *password*
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** *phone-tag* **Example:** `Router(config)# ephone 2`	Enters ephone configuration mode.
Step 4	**username** *username* **password** *password* **Example:** `Router(config-ephone)# username prx password pk59wq`	Assigns a phone user login account name and password. • This allows the phone user to log in to the Cisco Unified CME GUI to change a limited number of personal settings. • *username*—Unique alphanumeric string to identify a user for this authentication credential only.

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

Troubleshooting the GUI

If you are having trouble starting the Cisco Unified CME GUI, try the following actions:

Step 1 Verify you are using Microsoft Internet Explorer 5.5 or a later version. No other browser is supported.

Step 2 Clear your browser cache or history.

Step 3 Verify that the GUI files in router flash memory are the correct version for the version of Cisco Unified CME that you have. Compare the filenames in flash memory with the list in the Cisco Unified CME software archive that you downloaded. Compare the sizes of files in flash memory with the sizes of the files in the tar archive for the Cisco Unified CME GUI to ensure that you have the most recent files installed in flash memory. If necessary, download the latest version from the Software Download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Configuration Examples for Enabling the GUI

Example for Configuring HTTP Server and System Administrator Account

The following example sets up the HTTP server and creates a system administrator account for pwa3, a customer administrator account for user44, and a user account for prx.

```
ip http server
ip http path flash:
ip http authentication aaa

telephony-service
 web admin system name pwa3 secret 0 wp78pw
 web admin customer name user44 password pw10293847
 dn-webedit
 time-webedit

ephone 25
 username prx password pswd
```

Example for Configuring XML Configuration File Template

```
<Presentation>
```

```
 <MainMenu>
   <!-- Take Higher Precedence over CLI "dn-web-edit" -->
   <AddExtension> [Hide | Show] </AddExtension>
   <DeleteExtension> [Hide | Show] </DeleteExtension>
   <AddPhone> [Hide | Show] </AddPhone>
   <DeletePhone> [Hide | Show] </DeletePhone>
 </MainMenu>

 <Extension>
   <!-- Control both view and change, and possible add or delete -->
   <SequenceNumber> [Hide | Show] </SequenceNumber>
   <Type> [Hide | Show] </Type>
   <Huntstop> [Hide | Show] </Huntstop>
   <Preference> [Hide | Show] </Preference>
   <HoldAlert> [Hide | Show] </HoldAlert>
   <TranslationRules> [Hide | Show] </TranslationRules>
   <Paging> [Hide | Show] </Paging>
   <Intercom> [Hide | Show] </Intercom>
   <MWI> [Hide | Show] </MWI>
   <MoH> [Hide | Show] </MoH>
   <LBDN> [Hide | Show] </LBDN>
   <DualLine> [Hide | Show] </DualLine>
   <Reg> [Hide | Show] </Reg>
   <PGroup> [Hide | Show] </PGroup>
 </Extension>

 <Phone>
   <!-- control both view and change, and possible add and delete --->
   <SequenceNumber> [Hide | Show] </SequenceNumber>
 </Phone>

 <System>
   <!-- Control View Only -->
   <PhoneURL> [Hide | Show] </PhoneURL>
   <PhoneLoad> [Hide | Show]</PhoneLoad>
   <CallHistory> [Hide | Show] </CallHistory>
   <MWIServer> [Hide | Show] </MWIServer>
   <!-- Control Either View and Change or Change Only -->
   <TransferPattern attr=[Both | Change]> [Hide | Show] </TransferPattern>
   <VoiceMailNumber attr=[Both | Change]> [Hide | Show] </VoiceMailNumber>
   <MaxNumberPhone attr=[Both | Change]> [Hide | Show] </MaxNumberPhone>
   <DialplanPattern attr=[Both | Change]> [Hide | Show] </DialplanPattern>
   <SecDialTone attr=[Both | Change]> [Hide | Show] </SecDialTone>
   <Timeouts attr=[Both | Change]> [Hide | Show] </Timeouts>
   <CIDBlock attr=[Both | Change]> [Hide | Show] </CIDBlock>
   <HuntGroup attr=[Both | Change]> [Hide | Show] </HuntGroup>
   <NightSerBell attr=[Both | Change]> [Hide | Show] </NightSerBell>
   <!-- Control Change Only -->
   <!-- Take Higher Precedence over CLI "time-web-edit" -->
   <Time> [Hide | Show] </Time>
 </System>
 <Function>
   <AddLineToPhone> [No | Yes] </AddLineToPhone>
   <DeleteLineFromPhone> [No | Yes] </DeleteLineFromPhone>
   <NewDnDpCheck> [No | Yes] </NewDnDpCheck>
   <MaxLinePerPhone> [1-6] </MaxLinePerPhone>
 </Function>
</Presentation>
```

Example for Configuring XML Configuration File

```
sample.xml
<Presentation>
  <MainMenu>
   <AddExtension> Hide </AddExtension>
   <DeleteExtension> Hide </DeleteExtension>
   <AddPhone> Hide </AddPhone>
   <DeletePhone> Hide </DeletePhone>
```

```
  </MainMenu>
  <Extension>
   <SequenceNumber> Hide </SequenceNumber>
   <Type> Hide </Type>
   <Huntstop> Hide </Huntstop>
   <Preference> Hide </Preference>
   <HoldAlert> Hide </HoldAlert>
   <TranslationRule> Hide </TranslationRule>
   <Paging> Show </Paging>
   <Intercom> Hide </Intercom>
   <MWI> Hide </MWI>
   <MoH> Hide </MoH>
   <LBDN> Hide </LBDN>
   <DualLine> Hide </DualLine>
   <Reg> Hide </Reg>
   <PGroup> Show </PGroup>
  </Extension>

  <Phone>
   <SequenceNumber> Hide </SequenceNumber>
  </Phone>

  <System>
   <PhoneURL> Hide </PhoneURL>
   <PhoneLoad> Hide </PhoneLoad>
   <CallHistory> Hide </CallHistory>
   <MWIServer> Hide </MWIServer>
   <TransferPattern attr=Both> Hide </TransferPattern>
   <VoiceMailNumber attr=Both> Hide </VoiceMailNumber>
   <MaxNumberPhone attr=Both> Hide </MaxNumberPhone>
   <DialplanPattern attr=Change> Hide </DialplanPattern>
   <SecDialTone attr=Both> Hide </SecDialTone>
   <Timeouts attr=Both> Hide </Timeouts>
   <CIDBlock attr=Both> Hide </CIDBlock>
   <HuntGroup attr=Change> Hide </HuntGroup>
   <NightSerBell attr=Change> Hide </NightSerBell>
   <Time> Hide </Time>
  </System>

  <Function>
   <AddLineToPhone> No </AddLineToPhone>
   <DeleteLineFromPhone> No </DeleteLineFromPhone>
   <MaxLinePerPhone> 4 </MaxLinePerPhone>
  </Function>
</Presentation>
```

Feature Information for Enabling the GUI

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

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

Table 37: Feature Information for Enabling the GUI

Feature Name	Cisco Unified CME Version	Feature Information
Support for Extension Mobility Phone Users in Cisco Unified CME GUI	4.2(1)	Allows a phone user to use a name and password from an Extension Mobility profile to log into the Cisco Unified CME GUI for configuring personal speed dials on an Extension Mobility phone.
Cisco Unified CME GUI	2.0	The Cisco Unified CME GUI was introduced.

CHAPTER 16

Voice Mail Integration

This chapter describes how to integrate your voice-mail system with Cisco Unified Communications Manager Express (Cisco Unified CME).

Prerequisites for Voice Mail Integration

- Calls can be successfully completed between phones on the same Cisco Unified CME router.
- If your voice-mail system is something other than Cisco Unified Express, such as Cisco Unity, voice mail must be installed and configured on your network.
- If your voice-mail system is Cisco Unity Express:

Note When you order Cisco Unity Express, Cisco Unity Express software and the purchased license are installed on the module at the factory. Spare modules also ship with the software and license installed. If you are adding Cisco Unity Express to an existing Cisco router, you will be required to install hardware and software components.

  - Interface module for Cisco Unity Express is installed. For information about the AIM-CUE or NM-CUE, access documents located at http://www.cisco.com/en/US/products/hw/modules/ps2797/prod_installation_guides_list.html.
  - The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware and GUI files to support Cisco Unity Express are installed on the Cisco Unified CME router.

    If the GUI files are not installed, see Install Cisco Unified CME Software.

To determine whether the Cisco IOS software release and Cisco Unified CME software version are compatible with the Cisco Unity Express version, Cisco router model, and Cisco Unity Express hardware that you are using, see Cisco Unity Express Compatibility Matrix.

To verify installed Cisco Unity Express software version, enter the Cisco Unity Express command environment and use the **show software version** user EXEC command. For information about the command environment, see the appropriate *Cisco Unity Express CLI Administrator Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/roadmap/cuedocs.html.

- The proper license for Cisco Unified CME, not Cisco Unified Communications Manager, is installed. To verify installed license, enter the Cisco Unity Express command environment and use the **show software license** user EXEC command. For information about the command environment, see the appropriate *Cisco Unity Express CLI Administrator Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/roadmap/cuedocs.html.

  This is an example of the Cisco Unified CME license:

```
se-10-0-0-0> show software licenses
Core:
- application mode: CCME
- total usable system ports: 8

Voicemail/Auto Attendant:
- max system mailbox capacity time: 6000
- max general delivery mailboxes: 15
- max personal mailboxes: 50

Languages:
- max installed languages: 1
- max enabled languages: 1
```

- Voicemail and Auto Attendant (AA) applications are configured. For configuration information, see "*Configuring the System Using the Initialization Wizard*" in the appropriate Cisco Unity Express GUI Administrator Guide at http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/roadmap/cuedocs.html.

Information About Voice-Mail Integration

Cisco Unity Connection Integration

Cisco Unity Connection transparently integrates messaging and voice recognition components with your data network to provide continuous global access to calls and messages. These advanced, convergence-based communication services help you use voice commands to place calls or listen to messages in "hands-free" mode and check voice messages from your desktop, either integrated into an e-mail inbox or from a Web browser. Cisco Unity Connection also features robust automated-attendant functions that include intelligent routing and easily customizable call-screening and message-notification options.

For instructions on how to integrate Cisco Unified CME with Cisco Unity Connection, see Cisco CallManager Express 3.x Integration Guide for Cisco Unity Connection 1.1.

Cisco Unity Express Integration

Cisco Unity Express offers easy, one-touch access to messages and commonly used voice-mail features that enable users to reply, forward, and save messages. To improve message management, users can create alternate greetings, access envelope information, and mark or play messages based on privacy or urgency. For instructions on how to configure Cisco Unity Express, see the administrator guides for Cisco Unity Express.

For configuration information, see Enable DTMF Integration Using SIP NOTIFY.

Note Cisco Unified CME and Cisco Unity Express must both be configured before they can be integrated.

Cisco Unity Integration

Cisco Unity is a Microsoft Windows-based communications solution that brings you voice mail and unified messaging and integrates them with the desktop applications you use daily. Cisco Unity gives you the ability to access all of your messages, voice, fax, and e-mail, by using your desktop PC, a touchtone phone, or the Internet. The Cisco Unity voice mail system supports voice-mail integration with Cisco Unified CME. This integration requires that you configure the Cisco Unified CME router and Cisco Unity software to get voice-mail service.

For configuration instructions, see Enable DTMF Integration Using RFC 2833.

DTMF Integration for Legacy Voice-Mail Applications

For dual-tone multifrequency (DTMF) integrations, information on how to route incoming or forwarded calls is sent by a telephone system in the form of DTMF digits. The DTMF digits are sent in a pattern that is based on the integration file in the voice-mail system connected to the Cisco Unified CME router. These patterns are required for DTMF integration of Cisco Unified CME with most voice-mail systems. Voice-mail systems are designed to respond to DTMF after the system answers the incoming calls.

After configuring the DTMF integration patterns on the Cisco Unified CME router, you set up the integration files on the third-party legacy voice-mail system by following the instructions in the documents that accompany the voice-mail system. You must design the DTMF integration patterns appropriately so that the voice-mail system and the Cisco Unified CME router work with each other.

For configuration information, see Enable DTMF Integration for Analog Voice-Mail Applications.

Mailbox Selection Policy

Typically a voice-mail system uses the number that a caller has dialed to determine the mailbox to which a call should be sent. However, if a call has been diverted several times before reaching the voice-mail system, the mailbox that is selected might vary for different types of voice-mail systems. For example, Cisco Unity Express uses the last number to which the call was diverted before it was sent to voice mail as the mailbox number. Cisco Unity and some legacy PBX systems use the originally called number as the mailbox number.

The Mailbox Selection Policy feature allows you to provision the following options from the Cisco Unified CME configuration.

- For Cisco Unity Express, you can select the originally dialed number.
- For PBX voice-mail systems, you can select the last number to which the call was diverted before it was sent to voice mail. This option is configured on the outgoing dial peer for the voice-mail system's pilot number.
- For Cisco Unity voice mail, you can select the last number to which the call was diverted before it was sent to voice mail. This option is configured on the ephone-dn that is associated with the voice-mail pilot number.

To enable Mailbox Selection Policy, see Set a Mailbox Selection Policy for Cisco Unity Express or a PBX Voice-Mail Number or Set a Mailbox Selection Policy for Cisco Unity.

RFC 2833 DTMF MTP Pass through

In Cisco Unified CME 4.1, the RFC 2833 Dual-Tone Multifrequency (DTMF) Media Termination Point (MTP) Passthrough feature provides the capability to pass DTMF tones transparently between SIP endpoints that require transcoding or Resource Reservation Protocol (RSVP) agents.

This feature supports DTMF Relay across SIP WAN devices that support RFC 2833, such as Cisco Unity and SIP trunks. Devices registered to a Cisco Unified CME SIP back-to-back user agent (B2BUA) can exchange RFC 2833 DTMF MTP with other devices that are not registered with the Cisco Unified CME SIP B2BUA, or with devices that are registered in one of the following:

- Local or remote Cisco Unified CME
- Cisco Unified Communications Manager
- Third party proxy

By default, the RFC 2833 DTMF MTP Passthrough feature uses payload type 101 on MTP, and MTP accepts all the other dynamic payload types if it is indicated by Cisco Unified CME. For configuration information, see Enable DTMF Integration Using RFC 2833.

MWI Line Selection

Message waiting indicator (MWI) line selection allows you to choose the phone line that is monitored for voice-mail messages and that lights an indicator when messages are present.

Before Cisco Unified CME 4.0, the MWI lamp on a phone running SCCP could be associated only with the primary line of the phone.

In Cisco Unified CME 4.0 and later versions, you can designate a phone line other than the primary line to be associated with the MWI lamp. Lines other than the one associated with the MWI lamp display an envelope icon when a message is waiting. A logical phone “line” is not the same as a phone button. A button with one or more directory numbers is considered one line. A button with no directory number assigned does not count as a line.

In Cisco Unified CME 4.0 and later versions, a SIP directory number that is used for call forward all, presence BLF status, and MWI features must be configured by using the **dn** keyword in the **number** command; direct line numbers are not supported.

For configuration information, see Configure a Voice Mailbox Pilot Number on a SCCP Phone or Configure a Directory Number for MWI NOTIFY.

AMWI

The AMWI (Audible Message Line Indicator) feature provides a special stutter dial tone to indicate message waiting. This is an accessibility feature for vision-impaired phone users. The stutter dial tone is defined as 10 ms ON, 100 ms OFF, repeat 10 times, then steady on.

In Cisco Unified CME 4.0(3), you can configure the AMWI feature on the Cisco Unified IP Phone 7911 and Cisco Unified IP Phone 7931G to receive audible, visual, or audible and visual MWI notification from an external voice-messaging system. AMWI cannot be enabled unless the **number** command is already configured for the IP phone to be configured.

Cisco Unified CME applies the following logic based on the capabilities of the IP phone and how MWI is configured:

- If the phone supports (visual) MWI and MWI is configured for the phone, activate the Message Waiting light.
- If the phone supports (visual) MWI only, activate the Message Waiting light regardless of the configuration.
- If the phone supports AMWI and AMWI is configured for the phone, send the stutter dial tone to the phone when it goes off-hook.
- If the phone supports AMWI only and AMWI is configured, send the stutter dial tone to the phone when it goes off-hook regardless of the configuration.

If a phone supports (visual) MWI and AMWI and both options are configured for the phone, activate the Message Waiting light and send the stutter dial tone to the phone when it goes off-hook.

For configuration information, see Configure a SCCP Phone for MWI Outcall.

SIP MWI Prefix Specification

Central voice-messaging servers that provide mailboxes for several Cisco Unified CME sites may use site codes or prefixes to distinguish among similarly numbered ranges of extensions at different sites. In Cisco Unified CME 4.0 and later versions, you can specify that your Cisco Unified CME system should accept unsolicited SIP Notify messages for MWI that include a prefix string as a site identifier.

For example, an MWI message might indicate that the central mailbox number 555-0123 has a voice message. In this example, the digits 555 are set as the prefix string or site identifier using the **mwi prefix** command. The local Cisco Unified CME system is able to convert 555-0123 to 0123 and deliver the MWI to the correct phone. Without this prefix string manipulation, the system would reject an MWI for 555-0123 as not matching the local Cisco Unified CME extension 0123.

To enable SIP MWI Prefix Specification, see Enable SIP MWI Prefix Specification.

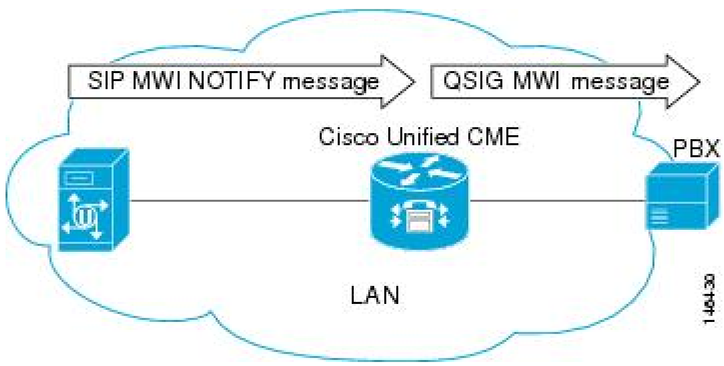
SIP MWI - QSIG Translation

In Cisco Unified CME 4.1 and later, the SIP MWI - QSIG Translation feature extends MWI functionality for SIP MWI and QSIG MWI interoperation to enable sending and receiving MWI over QSIG to a PBX.

When the SIP Unsolicited NOTIFY is received from voice mail, the Cisco router translates this event to activate QSIG MWI to the PBX, via PSTN. The PBX will switch on, or off, the MWI lamp on the corresponding IP phone. This feature supports only Unsolicited NOTIFY. Subscribe NOTIFY is not supported by this feature.

In Figure 18: SIP MWI to ISDN QSIG When Voice Mail and Cisco Router are On the Same LAN, on page 544, the Cisco router receives the SIP Unsolicited NOTIFY, performs the protocol translation, and initiates the QSIG MWI call to the PBX, where it is routed to the appropriate phone.

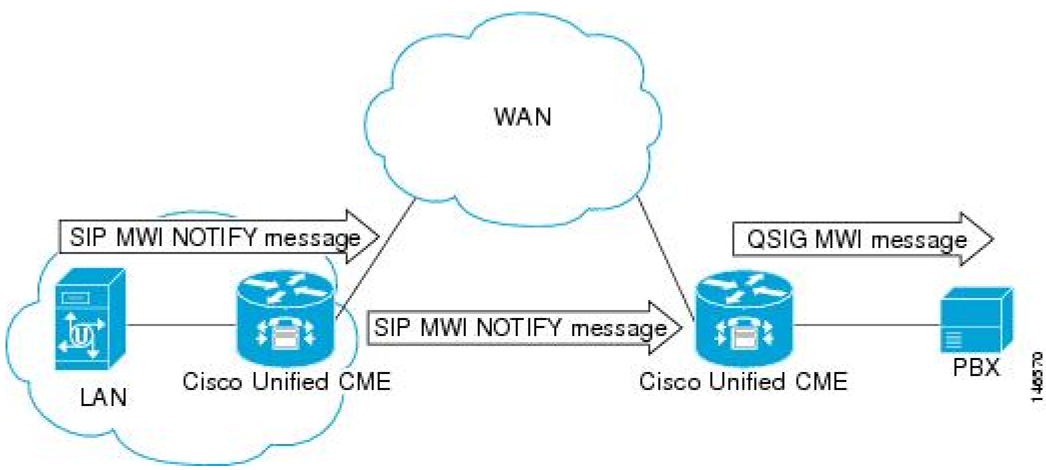
Figure 18: SIP MWI to ISDN QSIG When Voice Mail and Cisco Router are On the Same LAN



It makes no difference if the SIP Unsolicited NOTIFY is received via LAN or WAN if the PBX is connected to the Cisco router, and not to the remote voice-mail server.

In Figure 19: SIP MWI to ISDN QSIG When PBX is Connected to a Remote Cisco Router, on page 544, a voice mail server and Cisco Unified CME are connected to the same LAN and a remote Cisco Unified CME is connected across the WAN. In this scenario, the protocol translation is performed at the remote Cisco router and the QSIG MWI message is sent to the PBX.

Figure 19: SIP MWI to ISDN QSIG When PBX is Connected to a Remote Cisco Router



VMWI

There are two types of visual message waiting indicator (VMWI) features: Frequency-shift Keying (FSK) and DC voltage. The message-waiting lamp can be enabled to flash on an analog phone that requires an FSK message to activate a visual indicator. The DC Voltage VMWI feature is used to flash the message-waiting lamp on an analog phone which requires DC voltage instead of an FSK message. For all other applications, such as MGCP, FSK VMWI is used even if the voice gateway is configured for DC voltage VMWI. The configuration for DC voltage VMWI is supported only for Foreign Exchange Station (FXS) ports on the Cisco VG224 analog voice gateway with analog device version V1.3 and V2.1.

The Cisco VG224 can only support 12 Ringer Equivalency Number (REN) for ringing 24 onboard analog FXS voice ports. To support ringing and DC Voltage VMWI for 24 analog voice ports, stagger-ringing logic is used to maximize the limited REN resource. When a system runs out of REN because too many voice ports are being rung, the MWI lamp temporarily turns off to free up REN to ring the voice ports.

DC voltage VMWI is also temporarily turned off any time the port's operational state is no longer idle and onhook, such as when one of the following events occur:

- Incoming call on voice port
- Phone goes off hook
- The voice port is shut down or busied out

Once the operational state of the port changes to idle and onhook again, the MWI lamp resumes flashing until the application receives a requests to clear it; for example, if there are no more waiting messages.

For configuration information, see Transfer to Voice Mail.

Transfer to Voice Mail

The Transfer to Voice Mail feature allows a phone user to transfer a caller directly to a voice-mail extension. The user presses the TrnsfVM softkey to place the call on hold, enters the extension number, and then commits the transfer by pressing the TrnsfVM softkey again. The caller hears the complete voice mail greeting. This feature is supported using the TrnsfVM softkey or feature access code (FAC).

For example, a receptionist might screen calls for five managers. If a call comes in for a manager who is not available, the receptionist can transfer the caller to the manager's voice-mail extension by using the TrnsfVM softkey and the caller hears the personal greeting of the individual manager.

For configuration information, see Transfer to Voice Mail.

Live Record

The Live Record feature enables IP phone users in a Cisco Unified CME system to record a phone conversation if Cisco Unity Express is the voice mail system. An audible notification, either by announcement or by periodic beep, alerts participants that the conversation is being recorded. The playing of the announcement or beep is under the control of Cisco Unity Express.

Live Record is supported for two-party calls and ad hoc conferences. In normal record mode, the conversation is recorded after the LiveRcd softkey is pressed. This puts the other party on-hold and initiates a call to Cisco Unity Express at the configured live-record number. To stop the recording session, the phone user presses the LiveRcd softkey again, which toggles between on and off.

The Live-Record number is configured globally and must match the number configured in Cisco Unity Express. You can control the availability of the feature on individual phones by modifying the display of the LiveRcd softkey using an ephone template. This feature must be enabled on both Cisco Unified CME and Cisco Unity Express.

To enable Live Record in Cisco Unified CME, see Configure Live Record on SCCP Phones.

Cisco Unity Express AXL Enhancement

In Cisco Unified CME 7.0(1) and later versions, the Cisco Unity Express AXL enhancement in Cisco Unified CME provides better administrative integration between Cisco Unified CME and Cisco Unity Express by automatically synchronizing passwords.

No configuration is required to enable this feature.

Configure Voice-Mail Integration

Configure a Voice Mailbox Pilot Number on a SCCP Phone

To configure the telephone number that is speed-dialed when the Message button on a SCCP phone is pressed, perform the following steps.

Note The same telephone number is configured for voice messaging for all SCCP phones in Cisco Unified CME.

Before You Begin

- Voicemail phone number must be a valid number; directory number and number for voicemail phone number must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **voicemail** *phone-number*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters voice register global configuration mode to set parameters for all supported phones in Cisco Unified CME.
Step 4	**voicemail** *phone-number* **Example:** `Router(config-telephony)# voice mail 0123`	Defines the telephone number that is speed-dialed when the Messages button on a Cisco Unified IP phone is pressed. • *phone-number*—Same phone number is configured for voice messaging for all SCCP phones in a Cisco Unified CME.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

What to Do Next

- (Cisco Unified CME 4.0 or a later version only) To set up a mailbox selection policy, see Configure a Mailbox Selection Policy on SCCP Phone.
- To set up DTMF integration patterns for connecting to analog voice-mail applications, see Enable DTMF Integration for Analog Voice-Mail Applications.
- To connect to a remote SIP-based IVR or Cisco Unity, or to connect to a remote SIP-PSTN that goes through the PSTN to a voice-mail or IVR application, see Enable DTMF Integration Using RFC 2833.
- To connect to a Cisco Unity Express system, configure a nonstandard SIP NOTIFY format. See Enable DTMF Integration Using SIP NOTIFY.

Configure a Mailbox Selection Policy on SCCP Phone

Perform *one* of the following tasks, depending on which voice-mail application is used:

- Set a Mailbox Selection Policy for Cisco Unity Express or a PBX Voice-Mail Number
- Set a Mailbox Selection Policy for Cisco Unity

Set a Mailbox Selection Policy for Cisco Unity Express or a PBX Voice-Mail Number

To set a policy for selecting a mailbox for calls from a Cisco Unified CME system that are diverted before being sent to a Cisco Unity Express or PBX voice-mail pilot number, perform the following steps.

Restriction In the following scenarios, the mailbox selection policy can fail to work properly:

- The last redirecting endpoint is not hosted on Cisco Unified CME. This may rarely occur with a PBX.
- A call is forwarded across several SIP trunks. Multiple SIP Diversion Headers (stacking hierarchy) are not supported in Cisco IOS software.
- A call is forwarded across non-Cisco voice gateways that do not support the optional H450.3 originalCalledNr field.

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip** or **dial-peer voice** *tag* **pots**
4. **mailbox-selection** [**last-redirect-num** | **orig-called-num**]
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* **voip** or **dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 7000 voip`	Enters dial-peer configuration mode. • *tag*—identifies the dial peer. Valid entries are 1 to 2147483647. **Note** Use this command on the outbound dial peer associated with the pilot number of the voice-mail system. For systems using Cisco Unity Express, this is a VoIP dial peer. For systems using PBX-based voice mail, this is a POTS dial peer.

	Command or Action	Purpose
	or `Router(config)# dial-peer voice 35 pots`	
Step 4	**mailbox-selection** [**last-redirect-num** | **orig-called-num**] **Example:** `Router(config-dial-peer)# mailbox-selection orig-called-num`	Sets a policy for selecting a mailbox for calls that are diverted before being sent to a voice-mail line. • **last-redirect-num**—(PBX voice mail only) The mailbox number to which the call will be sent is the last number to divert the call (the number that sends the call to the voice-mail pilot number). • **orig-called-num**—(Cisco Unity Express only) The mailbox number to which the call will be sent is the number that was originally dialed before the call was diverted.
Step 5	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

What to Do Next

- To use voice mail on a SIP network that connects to a Cisco Unity Express system, configure a nonstandard SIP NOTIFY format. See Enable DTMF Integration Using SIP NOTIFY.

Set a Mailbox Selection Policy for Cisco Unity

To set a policy for selecting a mailbox for calls that are diverted before being sent to a Cisco Unity voice-mail pilot number, perform the following steps.

Restriction This feature might not work properly in certain network topologies, including when:

- The last redirecting endpoint is not hosted on Cisco Unified CME. This may rarely occur with a PBX.
- A call is forwarded across several SIP trunks. Multiple SIP Diversion Headers (stacking hierarchy) are not supported in Cisco IOS software.
- A call is forwarded across other voice gateways that do not support the optional H450.3 originalCalledNr field.

Before You Begin

- Cisco Unified CME 4.0 or a later version.
- Directory number to be configured is associated with a voice mailbox.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **exit**
4. **ephone-dn** *dn-tag*
5. **mailbox-selection** [**last-redirect-num**]
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	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.
Step 4	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 752`	Enters ephone-dn configuration mode.
Step 5	**mailbox-selection** [**last-redirect-num**] **Example:** `Router(config-ephone-dn)# mailbox-selection last-redirect-num`	Sets a policy for selecting a mailbox for calls that are diverted before being sent to a Cisco Unity voice-mail pilot number.
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

What to Do Next

- To use a remote SIP-based IVR or Cisco Unity, or to connect Cisco Unified CME to a remote SIP-PSTN that goes through the PSTN to a voice-mail or IVR application, see Enable DTMF Integration Using RFC 2833.

Transfer to Voice Mail

To enable a phone user to transfer a call to voice mail by using the TrnsfVM softkey or a FAC, perform the following steps.

Restriction The TrnsfVM softkey is not supported on the Cisco Unified IP Phone 7905, 7912, or 7921, or analog phones connected to the Cisco VG224 or Cisco ATA. These phones support the trnsfvm FAC.

Before You Begin

- Cisco Unified CME 4.3 or a later version.
- Cisco Unity Express 3.0 or a later version, installed and configured.
- For information about standard and custom FACs, see Feature Access Codes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]}
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
8. **exit**
9. **telephony-service**
10. **voicemail** *phone-number*
11. **fac** {**standard** | **custom trnsfvm** *custom-fac*}
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-template** *template-tag* **Example:** `Router(config)# ephone-template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template. Range: 1 to 20.
Step 4	**softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]} **Example:** `Router(config-ephone-template)# softkeys connected TrnsfVM Park Acct ConfList Confrn Endcall Trnsfer Hold`	(Optional) Modifies the order and type of softkeys that display on an IP phone during the connected call state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the ephone template that you created in Step 3, on page 552.
Step 8	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode.
Step 9	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 10	**voicemail** *phone-number* **Example:** `Router(config-telephony)# voicemail 8900`	Defines the telephone number that is speed-dialed when the Messages button on a Cisco Unified IP phone is pressed. • *phone-number*—Same phone number is configured for voice messaging for all SCCP phones in a Cisco Unified CME.
Step 11	**fac** {**standard** | **custom trnsfvm** *custom-fac*} **Example:** `Router(config-telephony)# fac custom trnsfvm #22`	Enables standard FACs or creates a custom FAC or alias. • **standard**—Enables standard FACs for all phones. Standard FAC for transfer to voice mail is *6. • **custom**—Creates a custom FAC for a FAC type. • *custom-fac*—User-defined code to be dialed using the keypad on an IP or analog phone. Custom FAC can be up to 256 characters long and contain numbers 0 to 9 and * and #.
Step 12	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

The following example shows a configuration where the display order of the TrnsfVM softkey is modified for the connected call state in ephone template 5 and assigned to ephone 12. A custom FAC for transfer to voice mail is set to #22.

```
telephony-service
 max-ephones 100
 max-dn 240
 timeouts transfer-recall 60
 voicemail 8900
 max-conferences 8 gain -6
 transfer-system full-consult
 fac custom trnsfvm #22
!
!
ephone-template  5
 softkeys connected  TrnsfVM Park Acct ConfList Confrn Endcall Trnsfer Hold
 max-calls-per-button 3
 busy-trigger-per-button 2
!
!
ephone  12
 ephone-template 5
 mac-address 000F.9054.31BD
 type 7960
 button  1:10 2:7
```

What to Do Next

- If you are finished modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for SCCP Phones.
- For information on how phone users transfer a call to voice mail, see Cisco Unified IP Phone documentation for Cisco Unified CME.

Configure Live Record on SCCP Phones

To configure the Live Record feature so that a phone user can record a conversation by pressing the LiveRcd softkey, perform the followings steps.

Restriction

- Only one live record session is allowed for each conference.
- Only the conference creator can initiate a live record session. In an ad hoc conference, participants who are not the conference creator cannot start a live record session. In a two-party call, the party who starts the live record session is the conference creator.

Note For legal disclaimer information about this feature, see copyright information section.

Before You Begin

- Cisco Unified CME 4.3 or a later version.
- Cisco Unity Express 3.0 or a later version, installed and configured. For information on configuring Live Record in Cisco Unity Express, see Configure Live Record in the *Cisco Unity Express Voice-Mail and Auto-Attendant CLI Administrator Guide for 3.0 and Later Versions*.
- Ad hoc hardware conference resource is configured and ready to use. See Configure Conferencing.
- If phone user wants to view the live record session, include ConfList softkey using the **softkeys** connected command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **live record** *number*
5. **voicemail** *number*
6. **exit**
7. **ephone-dn** *dn-tag*
8. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
9. **call-forward all** *target-number*
10. **exit**
11. **ephone-template** *template-tag*
12. **softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]}
13. **exit**
14. **ephone** *phone-tag*
15. **ephone-template** *template-tag*
16. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**live record** *number* **Example:** `Router(config-telephony)# live record 8900`	Defines the extension number that is dialed when the LiveRcd softkey is pressed on an SCCP IP phone.

	Command or Action	Purpose
Step 5	**voicemail** *number* **Example:** `Router(config-telephony)# voicemail 8000`	Defines the extension number that is speed-dialed when the Messages button is pressed on an IP phone. • *Number*—Cisco Unity Express voice-mail pilot number.
Step 6	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 7	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 10`	Creates a directory number that forwards all calls to the Cisco Unity Express voice-mail pilot number.
Step 8	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 8900`	Assigns an extension number to this directory number. • *Number*—Must match the Live Record pilot-number configured in Step 4, on page 555.
Step 9	**call-forward all** *target-number* **Example:** `Router(config-ephone-dn)# call-forward all 8000`	Forwards all calls to this extension to the specified voice-mail number. • *target-number*—Phone number to which calls are forwarded. Must match the voice-mail pilot number configured in Step 5, on page 556. **Note** Phone users can activate and cancel the call-forward-all state from the phone using the CFwdAll softkey or a FAC.
Step 10	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 11	**ephone-template** *template-tag* **Example:** `Router(config)# ephone-template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template. Range: 1 to 20.
Step 12	**softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]} **Example:** `Router(config-ephone-template)# softkeys connected LiveRcd Confrn Hold Park Trnsfer TrnsfVM`	Modifies the order and type of softkeys that display on an IP phone during the connected call state.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 14	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 15	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the ephone template that you created in Step 11, on page 556.
Step 16	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

The following example shows Live Record is enabled at the system-level for extension 8900. All incoming calls to extension 8900 are forwarded to the voice-mail pilot number 8000 when the LiveRcd softkey is pressed, as configured under ephone-dn 10. Ephone template 5 modifies the display order of the LiveRcd softkey on IP phones.

```
telephony-service
 privacy-on-hold
 max-ephones 100
 max-dn 240
 timeouts transfer-recall 60
 live-record 8900
 voicemail 8000
 max-conferences 8 gain -6
 transfer-system full-consult
 fac standard
!
!
ephone-template  5
 softkeys remote-in-use  CBarge Newcall
 softkeys hold  Resume Newcall Join
 softkeys connected  LiveRcd Confrn Hold Park Trnsfer TrnsfVM
 max-calls-per-button 3
 busy-trigger-per-button 2
!
!
ephone-dn  10
 number 8900
 call-forward all 8000
```

Configure a Voice Mailbox Pilot Number on a SIP Phone

To configure the telephone number that is speed-dialed when the Message button on a SIP phone is pressed, follow the steps in this section.

Note The same telephone number is configured for voice messaging for all SIP phones in Cisco Unified CME. The **call forward b2bua** command enables call forwarding and designates that calls that are forwarded to a busy or no-answer extension be sent to a voicemail box.

Before You Begin

- Directory number and number for voicemail phone number must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **voicemail** *phone-number*
5. **exit**
6. **voice register dn** *dn-tag*
7. **call-forward b2bua busy** *directory-number*
8. **call-forward b2bua mailbox** *directory-number*
9. **call-forward b2bua noan** *directory-number* **timeout** *seconds*
10. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**voicemail** *phone-number* **Example:** `Router(config-register-global)# voice mail 1111`	Defines the telephone number that is speed-dialed when the Messages button on a Cisco Unified IP phone is pressed. • *phone-number*—Same phone number is configured for voice messaging for all SIP phones in a Cisco Unified CME.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global configuration mode.
Step 6	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 2`	Enters voice register dn mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.
Step 7	**call-forward b2bua busy** *directory-number* **Example:** `Router(config-register-dn)# call-forward b2bua busy 1000`	Enables call forwarding for a SIP back-to-back user agent so that incoming calls to an extension that is busy will be forwarded to the designated directory number.
Step 8	**call-forward b2bua mailbox** *directory-number* **Example:** `Router(config-register-dn)# call-forward b2bua mailbox 2200`	Designates the voice mailbox to use at the end of a chain of call forwards. • Incoming calls have been forwarded to a busy or no-answer extension will be forwarded to the directory-number specified.
Step 9	**call-forward b2bua noan** *directory-number* **timeout** *seconds* **Example:** `Router(config-register-dn)# call-forward b2bua noan 2201 timeout 15`	Enables call forwarding for a SIP back-to-back user agent so that incoming calls to an extension that does not answer will be forwarded to the designated directory number. • *seconds*—Number of seconds that a call can ring with no answer before the call is forwarded to another extension. Range: 3 to 60000. Default: 20.
Step 10	**end** **Example:** `Router(config-register-dn)# end`	Exits to privileged EXEC mode.

What to Do Next

- To set up DTMF integration patterns for connecting to analog voice-mail applications, see Enable DTMF Integration for Analog Voice-Mail Applications.
- To use a remote SIP-based IVR or Cisco Unity, or to connect to a remote SIP-PSTN that goes through the PSTN to a voice-mail or IVR application, see Enable DTMF Integration Using RFC 2833.
- To connect to a Cisco Unity Express system, configure a nonstandard SIP NOTIFY format, see Enable DTMF Integration Using SIP NOTIFY.

Enable DTMF Integration

Perform *one* of the following tasks, depending on which DTMF-relay method is required:

- Enable DTMF Integration for Analog Voice-Mail Applications—To set up DTMF integration patterns for connecting to analog voice-mail applications.
- Enable DTMF Integration Using RFC 2833—To connect to a remote SIP-based IVR or voice-mail application such as Cisco Unity or when SIP is used to connect Cisco Unified CME to a remote SIP-PSTN voice gateway that goes through the PSTN to a voice-mail or IVR application.
- Enable DTMF Integration Using SIP NOTIFY—To configure a SIP dial peer to point to Cisco Unity Express.

Enable DTMF Integration for Analog Voice-Mail Applications

To set up DTMF integration patterns for analog voice-mail applications, perform the following steps.

Note You can configure multiple tags and tokens for each pattern, depending on the voice-mail system and type of access.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vm-integration**
4. **pattern direct** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]
5. **pattern ext-to-ext busy** *tag1* {**CGN** |**CDN** | **FDN**} [*tag2* {**CGN** | **CDN** |**FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]
6. **pattern ext-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** |**CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** |**FDN**}] [*last-tag*]
7. **pattern trunk-to-ext busy** *tag1* {**CGN** |**CDN** | **FDN**} [*tag2* {**CGN** | **CDN** |**FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*]
8. **pattern trunk-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** |**CDN** | **FDN**}] [*tag3* {**CGN** |**CDN** | **FDN**}] [*last-tag*]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vm-integration** **Example:** `Router(config) vm-integration`	Enters voice-mail integration configuration mode and enables voice-mail integration with DTMF and an analog voice-mail system.
Step 4	**pattern direct** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** | **CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-integration) 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. • The *tag* attribute is an 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. • The keywords, **CGN**, **CDN**, and **FDN**, configure the type of call information sent to the voice-mail system, such as calling number (CGN), called number (CDN), or forwarding number (FDN).
Step 5	**pattern ext-to-ext busy** *tag1* {**CGN** |**CDN** | **FDN**} [*tag2* {**CGN** | **CDN** |**FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-integration) pattern ext-to-ext busy 7 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when an internal extension attempts to connect to a busy extension and the call is forwarded to voice mail.
Step 6	**pattern ext-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** |**CDN** | **FDN**}] [*tag3* {**CGN** | **CDN** |**FDN**}] [*last-tag*] **Example:** `Router(config-vm-integration) pattern ext-to-ext no-answer 5 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when an internal extension fails to connect to an extension and the call is forwarded to voice mail.

	Command or Action	Purpose
Step 7	**pattern trunk-to-ext busy** *tag1* {**CGN** |**CDN** | **FDN**} [*tag2* {**CGN** | **CDN** |**FDN**}] [*tag3* {**CGN** | **CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-integration) pattern trunk-to-ext busy 6 FDN * CGN *`	Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when an external trunk call reaches a busy extension and the call is forwarded to voice mail.
Step 8	**pattern trunk-to-ext no-answer** *tag1* {**CGN** | **CDN** | **FDN**} [*tag2* {**CGN** |**CDN** | **FDN**}] [*tag3* {**CGN** |**CDN** | **FDN**}] [*last-tag*] **Example:** `Router(config-vm-integration)# 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.
Step 9	**end** **Example:** `Router(config-vm-integration)# exit`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

After configuring DTMF relay, you are ready to configure Message Waiting Indicator (MWI) notification for either the MWI outcall, unsolicited notify, or subscribe/notify mechanism. See Configure a SCCP Phone for MWI Outcall.

Enable DTMF Integration Using RFC 2833

To configure a SIP dial peer to point to Cisco Unity and enable SIP dual-tone multifrequency (DTMF) relay using RFC 2833, use the commands in this section on both the originating and terminating gateways.

This DTMF relay method is required in the following situations:

- When SIP is used to connect Cisco Unified CME to a remote SIP-based IVR or voice-mail application such as Cisco Unity.
- When SIP is used to connect Cisco Unified CME to a remote SIP-PSTN voice gateway that goes through the PSTN to a voice-mail or IVR application.

Note If the T.38 Fax Relay feature is also configured on this IP network, we recommend that you either configure the voice gateways to use a payload type other than PT96 or PT97 for fax relay negotiation, or depending on whether the SIP endpoints support different payload types, configure Cisco Unified CME to use a payload type other than PT96 or PT97 for DTMF.

Before You Begin

- Configure the **codec** or **voice-class codec** command for transcoding between G.711 and G.729.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **description** *string*
5. **destination-pattern** *string*
6. **session protocol sipv2**
7. **session target** {**dns**:*address* | **ipv4**:*destination-address*}
8. **dtmf-relay rtp-nte**
9. **dtmf-interworking rtp-nte**
10. **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* **voip** **Example:** `Router (config)# dial-peer voice 123 voip`	Enters dial-peer configuration mode to define a VoIP dial peer for the voice-mail system. • *tag*—Defines the dial peer being configured. Range is 1 to 2147483647.
Step 4	**description** *string* **Example:** `Router (config-voice-dial-peer)# description CU pilot`	(Optional) Associates a description with the dial peer being configured. Enter a string of up to 64 characters.
Step 5	**destination-pattern** *string* **Example:** `Router (config-voice-dial-peer)# destination-pattern 20`	Specifies the pattern of the numbers that the user must dial to place a call. • *string*—Prefix or full E.164 number.

	Command or Action	Purpose
Step 6	**session protocol sipv2** **Example:** `Router (config-voice-dial-peer)# session protocol sipv2`	Specifies that Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP) is protocol to be used for calls between local and remote routers using the packet network.
Step 7	**session target** {**dns**:*address* | **ipv4**:*destination-address*} **Example:** `Router (config-voice-dial-peer)# session target ipv4:10.8.17.42`	Designates a network-specific address to receive calls from the dial peer being configured. • **dns**:*address*—Specifies the DNS address of the voice-mail system. • **ipv4**:*destination- address*—Specifies the IP address of the voice-mail system.
Step 8	**dtmf-relay rtp-nte** **Example:** `Router (config-voice-dial-peer)# dtmf-relay rtp-nte`	Sets DTMF relay method for the voice dial peer being configured. • **rtp-nte**— Provides conversion from the out-of-band SCCP indication to the SIP standard for DTMF relay (RFC 2833). Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type. • This command can also be configured in voice-register-pool configuration mode. For individual phones, the phone-level configuration for this command overrides the system-level configuration for this command. **Note** The need to use out-of-band conversion is limited to SCCP phones. SIP phones natively support in-band.
Step 9	**dtmf-interworking rtp-nte** **Example:** `Router (config-voice-dial-peer)# dtmf-interworking rtp-nte`	(Optional) Enables a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets. • This command is supported in Cisco IOS Release 12.4(15)XZ and later releases and in Cisco Unified CME 4.3 and later versions. • This command can also be configured in voice-service configuration mode.
Step 10	**end** **Example:** `Router(config-voice-dial-peer)# end`	Exits to privileged EXEC mode.

What to Do Next

After configuring DTMF relay, you are ready to configure Message Waiting Indicator (MWI) notification for either the MWI outcall, unsolicited notify, or subscribe/notify mechanism. See Configure a SCCP Phone for MWI Outcall.

Enable DTMF Integration Using SIP NOTIFY

To configure a SIP dial peer to point to Cisco Unity Express and enable SIP dual-tone multi-frequency (DTMF) relay using SIP NOTIFY format, follow the steps in this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **description** *string*
5. **destination-pattern** *string*
6. **b2bua**
7. **session protocol sipv2**
8. **session target** {**dns**:*address* | **ipv4**:*destination-address*}
9. **dtmf-relay sip-notify**
10. **codec** *g711ulaw*
11. **no vad**
12. **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* **voip** **Example:** `Router (config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode to define a VoIP dial peer for the voice-mail system. • *tag*—Defines the dial peer being configured. Range is 1 to 2147483647.
Step 4	**description** *string* **Example:** `Router (config-voice-dial-peer)# description cue pilot`	(Optional) Associates a description with the dial peer being configured. Enter a string of up to 64 characters.

	Command or Action	Purpose
Step 5	**destination-pattern** *string* **Example:** `Router (config-voice-dial-peer)# destination-pattern 20`	Specifies the pattern of the numbers that the user must dial to place a call. • *string*—Prefix or full E.164 number.
Step 6	**b2bua** **Example:** `Router (config-voice-dial-peer)# b2bua`	(Optional) Includes the Cisco Unified CME address as part of contact in 3XX response to point to Cisco Unity Express and enables SIP-to-SCCP call forward.
Step 7	**session protocol sipv2** **Example:** `Router (config-voice-dial-peer)# session protocol sipv2`	Specifies that Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP) is protocol to be used for calls between local and remote routers using the packet network.
Step 8	**session target** {**dns**:*address* | **ipv4**:*destination-address*} **Example:** `Router (config-voice-dial-peer)# session target ipv4:10.5.49.80`	Designates a network-specific address to receive calls from the dial peer being configured. • **dns**:*address*—Specifies the DNS address of the voice-mail system. • **ipv4**:*destination- address*—Specifies the IP address of the voice-mail system.
Step 9	**dtmf-relay sip-notify** **Example:** `Router (config-voice-dial-peer)# dtmf-relay sip-notify`	Sets the DTMF relay method for the voice dial peer being configured. • **sip-notify**— Forwards DTMF tones using SIP NOTIFY messages. • This command can also be configured in voice-register-pool configuration mode. For individual phones, the phone-level configuration for this command overrides the system-level configuration for this command.
Step 10	**codec** *g711ulaw* **Example:** `Router (config-voice-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for a dial peer being configured.
Step 11	**no vad** **Example:** `Router (config-voice-dial-peer)# no vad`	Disables voice activity detection (VAD) for the calls using the dial peer being configured.
Step 12	**end** **Example:** `Router(config-voice-dial-peer)# end`	Exits to privileged EXEC mode.

What to Do Next

After configuring DTMF relay, you are ready to configure Message Waiting Indicator (MWI). See Configure a SCCP Phone for MWI Outcall.

Configure a SCCP Phone for MWI Outcall

To designate a phone line or directory number on an individual SCCP phone to be monitored for voice-mail messages, or to enable audible MWI, perform the following steps.

Restriction

- Audible MWI is supported only in Cisco Unified CME 4.0(2) and later versions.
- Audible MWI is supported only on Cisco Unified IP Phone 7931G and Cisco Unified IP Phone 7911.

Before You Begin

- Directory number and number for MWI line must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mwi-line** *line-number*
5. **exit**
6. **ephone-dn** *dn-tag*
7. **mwi** {**off** | **on** | **on-off**}
8. **mwi-type** {**visual** | **audio** | **both**}
9. **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.

	Command or Action	Purpose
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode.
Step 4	**mwi-line** *line-number* **Example:** `Router(config-ephone)# mwi-line 3`	(Optional) Selects a phone line to receive MWI treatment. • *line-number*—Number of phone line to receive MWI notification. Range: 1 to 34. Default: 1.
Step 5	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode.
Step 6	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 11`	Enters ephone-dn configuration mode.
Step 7	**mwi** {**off** | **on** | **on-off**} **Example:** `Router(config-ephone-dn)# mwi on-off`	(Optional) Enables a specific directory number to receive MWI notification from an external voice-messaging system. **Note** This command can also be configured in ephone-dn-template configuration mode. The value that you set in ephone-dn configuration mode has priority over the value set in ephone-dn-template mode.
Step 8	**mwi-type** {**visual** | **audio** | **both**} **Example:** `Router(config-ephone-dn)# mwi-type audible`	(Optional) Specifies which type of MWI notification to be received. **Note** This command is supported only on the Cisco Unified IP Phone 7931G and Cisco Unified IP Phone 7911. **Note** This command can also be configured in ephone-dn-template configuration mode. The value that you set in ephone-dn configuration mode has priority over the value set in ephone-dn-template mode. For configuration information, see Create an Ephone-dn Template.
Step 9	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Enable MWI at the System-Level on SIP Phones

To enable a message waiting indicator (MWI) at a system-level, perform the following steps.

Before You Begin

- Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mwi reg-e164**
5. **mwi stutter**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**mwi reg-e164** **Example:** `Router(config-register-global)# mwi reg-e164`	Registers full E.164 number to the MWI server in Cisco Unified CME and enables MWI.
Step 5	**mwi stutter** **Example:** `Router(config-register-global)# mwi stutter`	Enables Cisco Unified CME router at the central site to relay MWI notification to remote SIP phones.
Step 6	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Configure a Directory Number for MWI on SIP Phones

Perform *one* of the following tasks, depending on whether you want to configure MWI outcall or MWI notify (unsolicited notify or subscribe/notify) for SIP endpoints in Cisco Unified CME.

- Define Pilot Call Back Number for MWI Outcall
- Configure a Directory Number for MWI NOTIFY

Define Pilot Call Back Number for MWI Outcall

To designate a phone line on an individual SIP directory number to be monitored for voice-mail messages, perform the following steps.

Restriction

- For Cisco Unified CME 4.1 and later versions, the Call Forward All, Presence, and MWI features require that SIP phones must be configured with a directory number by using the **number** command with the **dn** keyword; direct line numbers are not supported.

Before You Begin

- Cisco CME 3.4 or a later version.
- Directory number and number for receiving MWI must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **mwi**
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.

	Command or Action	Purpose
Step 3	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.
Step 4	**mwi** **Example:** `Router(config-register-dn)# mwi`	Enables a specific directory number to receive MWI notification.
Step 5	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.

Configure a Directory Number for MWI NOTIFY

To identify the MWI server and specify a directory number for receiving MWI Subscribe/NOTIFY or MWI Unsolicited NOTIFY, follow the steps in this section.

Note We recommend using the Subscribe/NOTIFY method instead of an Unsolicited NOTIFY when possible.

Restriction

- For Cisco Unified CME 4.1 and later versions, the Call Forward All, Presence, and MWI features require that SIP phones must be configured with a directory number by using the **number** command with the **dn** keyword; direct line numbers are not supported.
- The SIP MWI - QSIG Translation feature in Cisco Unified CME 4.1 does not support Subscribe NOTIFY.
- Cisco Unified IP Phone 7960, 7940, 7905, and 7911 support only Unsolicited NOTIFY for MWI.

Before You Begin

- Cisco CME 3.4 or a later version.
- For Cisco Unified CME 4.0 and later, QSIQ supplementary services must be configured on the Cisco router. For information, see Enable H.450.7 and QSIG Supplementary Services at System-Level, on page 1202 or Enable H.450.7 and QSIG Supplementary Services on a Dial Peer, on page 1204.
- Directory number and number for receiving MWI must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **mwi-server** {**ipv4**:*destination-address* |**dns**:*host-name*} [**unsolicited**]
5. **exit**
6. **voice register dn** *dn-tag*
7. **mwi**
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	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters Session Initiation Protocol (SIP) user agent (ua) configuration mode for configuring the user agent.

Step 4	**mwi-server** {**ipv4**:*destination-address* |**dns**:*host-name*} [**unsolicited**]
	
	Example:
	`Router(config-sip-ua)# mwi-server ipv4:1.5.49.200`
	or
	`Router(config-sip-ua)# mwi-server dns:server.yourcompany.com unsolicited`
		Specifies voice-mail server settings on a voice gateway or UA.
		Note The **sip-server** and **mwi expires commands** under the telephony-service configuration mode have been migrated to **mwi-server** to support DNS format of the SIP server.

Step 5	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits to the next highest mode in the configuration mode hierarchy.
Step 6	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.

	Command or Action	Purpose
Step 7	**mwi** **Example:** `Router(config-register-dn)# mwi`	Enables a specific directory number to receive MWI notification.
Step 8	**end** **Example:** `Router(config-register-dn)# end`	Exits to privileged EXEC mode.

Enable SIP MWI Prefix Specification

To accept unsolicited SIP Notify messages for MWI that include a prefix string as a site identifier, perform the following steps.

Before You Begin

- Cisco Unified CME 4.0 or a later version.
- Directory number for receiving MWI Unsolicited NOTIFY must be configured. For information, see Configure a Directory Number for MWI NOTIFY.

SUMMARY STEPS

1. **enable**
2. **telephony-service**
3. **mwi prefix** *prefix-string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 3	**mwi prefix** *prefix-string* **Example:** `Router(config-telephony)# mwi prefix 555`	Specifies a string of digits that, if present before a known Cisco Unified CME extension number, are recognized as a prefix. • *prefix-string*—Digit string. The maximum prefix length is 32 digits.
Step 4	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure VMWI on SIP Phones

To enable a VMWI, perform the following steps.

Before You Begin

- Cisco IOS Release 12.4(6)T or a later version

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port*
4. **mwi**
5. **vmwi dc-voltage** or **vmwi fsk**
6. **exit**
7. **sip-ua**
8. **mwi-server** {**ipv4**:*destination-address* | **dns**:*host-name*} [**unsolicited**]
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice-port** *port* **Example:** `Router(config)# voice-port 2/0`	Enters voice-port configuration mode. • *port*—Syntax is platform-dependent. Type **?** to determine.
Step 4	**mwi** **Example:** `Router(config-voiceport)# mwi`	Enables MWI for a specified voice port.
Step 5	**vmwi dc-voltage** or **vmwi fsk** **Example:** `Router(config-voiceport)# vmwi dc-voltage`	(Optional) Enables DC voltage or FSK VMWI on a Cisco VG224 onboard analog FXS voice port. You do not need to perform this step for the Cisco VG202 and Cisco VG204. They support FSK only. VMWI is configured automatically when MWI is configured on the voice port. This step is required for the VG224. If an FSK phone is connected to the voice port, use the **fsk** keyword. If a DC voltage phone is connected to the voice port, use the **dc-voltage** keyword.
Step 6	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits to the next highest mode in the configuration mode hierarchy.
Step 7	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters Session Initiation Protocol user agent configuration mode for configuring the user agent.

Step 8	**mwi-server** {**ipv4**:*destination-address* | **dns**:*host-name*} [**unsolicited**]
	
	Example:
	`Router(config-sip-ua)# mwi-server ipv4:1.5.49.200`
	or
	`Router(config-sip-ua)# mwi-server dns:server.yourcompany.com unsolicited`
		Specifies voice-mail server settings on a voice gateway or user agent (ua).
		Note The **sip-server** and **mwi expires** commands under the telephony-service configuration mode have been migrated to **mwi-server** to support DNS format of the Session Initiation Protocol (SIP) server.

Step 9	**end** **Example:** `Router(config-voiceport)# end`	Exits voice-port configuration mode and returns to privileged EXEC mode.

Verify Voice-Mail Integration

- Press the **Messages** button on a local phone in Cisco Unified CME and listen for the voice mail greeting.
- Dial an unattended local phone and listen for the voice mail greeting.
- Leave a test message.
- Go to the phone that you called. Verify that the [Message] indicator is lit.
- Press the **Messages** button on this phone and retrieve the voice mail message.

Configuration Examples for Voice-Mail Integration

Example for Setting up a Mailbox Selection Policy for SCCP Phones

The following example sets a policy to select the mailbox of the originally called number when a call is diverted to a Cisco Unity Express or PBX voice-mail system with the pilot number 7000.

```
dial-peer voice 7000 voip
 destination-pattern 7000
 session target ipv4:10.3.34.211
 codec g711ulaw
 no vad
 mailbox-selection orig-called-num
```

The following example sets a policy to select the mailbox of the last number that the call was diverted to before being diverted to a Cisco Unity voice-mail system with the pilot number 8000.

```
ephone-dn 825
 number 8000
 mailbox-selection last-redirect-num
```

Example for Configuring Voice Mailbox for SIP Phones

The following example shows how to configure the call forward b2bua mailbox for SIP endpoints:

```
voice register global
   voicemail 1234
  !
  voice register dn 2
   number 2200
   call-forward b2bua all 1000
   call-forward b2bua mailbox 2200
   call-forward b2bua noan 2201 timeout 15
   mwi
```

Example for Configuring DTMF Integration Using RFC 2833

The following example shows the configuration for DTMF Relay using RFC 2833:

```
dial-peer voice 1 voip
   destination-pattern 4...
   session target ipv4:10.8.17.42
   session protocol sipv2
   dtmf-relay sip-notify rtp-nte
```

Example for Configuring DTMF Integration Using SIP Notify

The following example shows the configuration for DTMF using SIP Notify:

```
dial-peer voice 1 voip
   destination-pattern 4...
   session target ipv4:10.5.49.80
   session protocol sipv2
   dtmf-relay sip-notify
   b2bua
```

Example for Configuring DTMF Integration for Legacy Voice-Mail Applications

The following example sets up DTMF integration for an analog voice-mail system.

```
vm-integration
  pattern direct 2 CGN *
  pattern ext-to-ext busy 7 FDN * CGN *
  pattern ext-to-ext no-answer 5 FDN * CGN *
  pattern trunk-to-ext busy 6 FDN * CGN *
  pattern trunk-to-ext no-answer 4 FDN * CGN *
```

Example for Enabling SCCP Phone Line for MWI

The following example enables MWI on ephone 18 for line 2 (button 2), which has overlaid ephone-dns. Only a message waiting for the first ephone-dn (2021) on this line will activate the MWI lamp. Button 4 is unused. The line numbers in this example are as follows:

- Line 1—Button 1—Extension 2020
- Line 2—Button 2—Extension 2021, 2022, 2023, 2024
- Line 3—Button 3—Extension 2021, 2022, 2023, 2024 (rollover line)
- Button 4—Unused
- Line 4—Button 5—Extension 2025

```
ephone-dn 20
   number 2020

  ephone-dn 21
  number 2021

  ephone-dn 22
  number 2022

  ephone-dn 23
   number 2023
```

```
  ephone-dn 24
   number 2024

  ephone-dn 25
   number 2025

  ephone 18
  button 1:20 2o21,22,23,24,25 3x2 5:26
   mwi-line 2
```

The following example enables MWI on ephone 17 for line 3 (extension 609). In this example, the button numbers do not match the line numbers because buttons 2 and 4 are not used. The line numbers in this example are as follows:

- Line 1—Button 1—Extension 607
- Button 2—Unused
- Line 2—Button 3—Extension 608
- Button 4—Unused
- Line 3—Button 5—Extension 609

```
ephone-dn 17
   number 607

  ephone-dn 18
   number 608

  ephone-dn 19
   number 609

  ephone 25
   button 1:17 3:18 5:19
   mwi-line 3
```

Example for Configuring SIP MWI Prefix Specification

The following example identifies the SIP server for MWI notification at the IP address 172.16.14.22. It states that the Cisco Unified CME system will accept unsolicited SIP Notify messages for known mailbox numbers using the prefix 555.

```
sip-ua
   mwi-server 172.16.14.22 unsolicited

  telephony-service
   mwi prefix 555
```

Example for Configuring SIP Directory Number for MWI Outcall

The following example shows an MWI callback pilot number:

```
voice register dn
   number 9000….
   mwi
```

Example for Configuring SIP Directory Number for MWI Unsolicited Notify

The following example shows how to specify voice-mail server settings on a UA. The example includes the unsolicited keyword, enabling the voice-mail server to send a SIP notification message to the UA if the mailbox status changes and specifies that voice dn 1, number 1234 on the SIP phone in Cisco Unified CME will receive the MWI notification:

```
sip-ua
   mwi-server dns:server.yourcompany.com expires 60 port 5060 transport udp unsolicited

  voice register dn 1
  number 1234
  mwi
```

Example for Configuring SIP Directory Number for MWI Subscribe/NOTIFY

The following example shows how to define an MWI server and specify that directory number 1, number 1234 on a SIP phone in Cisco Unified CME is to receive the MWI notification:

```
sip-ua
   mwi-server ipv4:1.5.49.200

  voice register dn 1
  number 1234
  mwi
```

Feature Information for Voice-Mail Integration

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

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

Table 38: Feature Information for Voice-Mail Integration

Feature Name	Cisco Unified CME Version	Feature Information
Audible MWI	4.0(2)	Provides support for selecting audible, visual, or audible and visual Message Waiting Indicator (MWI) on supported Cisco Unified IP phones.
Cisco Unity Express AXL Enhancement	7.0(1)	Cisco Unified CME and Cisco Unity Express passwords are automatically synchronized. No configuration is required for this feature.

Feature Name	Cisco Unified CME Version	Feature Information
DTMF Integration	3.4	Added support for voice messaging systems connected via a SIP trunk or SIP user agent. The standard Subscribe/NOTIFY method is preferred over an Unsolicited NOTIFY.
	2.0	DTMF integration patterns were introduced.
Live Record	4.3	Enables IP phone users in a Cisco Unified CME system to record a phone conversation if Cisco Unity Express is the voice mail system.
Mailbox Selection Policy	4.0	Mailbox selection policy was introduced.
MWI	4.0	MWI line selection of a phone line other than the primary line on a SCCP phone was introduced.
	3.4	Voice messaging systems (including Cisco Unity) connected via a SIP trunk or SIP user agent can pass a Message Waiting Indicator (MWI) that will be received and understood by a SIP phone directly connected to Cisco Unified CME.
SIP MWI Prefix Specification	4.0	SIP MWI prefix specification was introduced.
SIP MWI - QSIG Translation	4.1	Extends message waiting indicator (MWI) functionality for SIP MWI and QSIG MWI interoperation to enable sending and receiving of MWI over QSIG to PBX.
Transfer to Voice Mail	4.3	Enables a phone user to transfer a caller directly to a voice-mail extension.

CHAPTER 17

Security

This chapter describes the phone authentication support in Cisco Unified Communications Manager Express (Cisco Unified CME), Hypertext Transfer Protocol Secure (HTTPS) provisioning for Cisco Unified IP Phones, and the Media Encryption (SRTP) on Cisco Unified CME feature that provides the following secure voice call capabilities:

- Secure call control signaling and media streams in Cisco Unified CME networks using Secure Real-Time Transport Protocol (SRTP) and H.323 protocols.
- Secure supplementary services for Cisco Unified CME networks using H.323 trunks.
- Secure Cisco VG224 Analog Phone Gateway endpoints.

Prerequisites for Security

- Cisco Unified CME 4.0 or a later version for Phone Authentication.
- Cisco Unified CME 4.2 or a later version for Media Encryption (SRTP) on Cisco Unified CME.
- Cisco IOS feature set Advanced Enterprise Services (adventerprisek9) or Advanced IP Services (advipservicesk9) on supported platforms.
- Firmware 9.0(4) or a later version must be installed on the IP phone for HTTPS provisioning.
- System clock must be set by using one of the following methods:

- ◦ Configure Network Time Protocol (NTP). For configuration information, see Enable Network Time Protocol, on page 133.
- ◦ Manually set the software clock using the **clock set** command. For information about this command, see Cisco IOS Network Management Command Reference.

Restrictions for Security

Phone Authentication

- Cisco Unified CME phone authentication is not supported on the Cisco IAD 2400 series or the Cisco 1700 series.

Media Encryption

- Secure three-way software conferencing is not supported. A secure call beginning with SRTP will always fall back to nonsecure Real-Time Transport Protocol (RTP) when it is joined to a conference.
- If a party drops from a three-party conference, the call between the remaining two parties returns to secure if the two parties are SRTP-capable local Skinny Client Control Protocol (SCCP) endpoints to a single Cisco Unified CME and the conference creator is one of the remaining parties. If either of the two remaining parties are only RTP-capable, the call remains nonsecure. If the two remaining parties are connected through FXS, PSTN, or VoIP, the call remains nonsecure.
- Calls to Cisco Unity Express are not secure.
- Music on Hold (MOH) is not secure.
- Video calls are not secure.
- Modem relay and T.3 fax relay calls are not secure.
- Media flow-around is not supported for call transfer and call forward.
- Conversion between inband tone and RFC 2833 DTMF is not supported. RFC 2833 DTMF handling is supported when encryption keys are sent to secure DSP Farm devices but is not supported for codec passthrough.
- Secure Cisco Unified CME supports SIP trunks and H.323 trunks.
- Secure calls are supported in the default session application only.

Information About Security

Phone Authentication Overview

Phone authentication is a security infrastructure for providing secure SCCP signaling between Cisco Unified CME and IP phones. The goal of Cisco Unified CME phone authentication is to create a secure environment for a Cisco Unified CME IP telephony system.

Phone authentication addresses the following security needs:

- Establishing the identity of each endpoint in the system
- Authenticating devices
- Providing signaling-session privacy
- Providing protection for configuration files

Cisco Unified CME phone authentication implements authentication and encryption to prevent identity theft of the phone or Cisco Unified CME system, data tampering, call-signaling tampering, or media-stream tampering. To prevent these threats, the Cisco Unified IP telephony network establishes and maintains authenticated communication streams, digitally signs files before they are transferred to phones, and encrypts call signaling between Cisco Unified IP phones.

Cisco Unified CME phone authentication depends on the following processes:

- Phone Authentication, on page 583
- File Authentication, on page 583
- Signaling Authentication, on page 583

Phone Authentication

The phone authentication process occurs between the Cisco Unified CME router and a supported device when each entity accepts the certificate of the other entity; only then does a secure connection between the entities occur. Phone authentication relies on the creation of a Certificate Trust List (CTL) file, which is a list of known, trusted certificates and tokens. Phones communicate with Cisco Unified CME using a Transport Layer Security (TLS) session connection, which requires that the following criteria be met:

- A certificate must exist on the phone.
- A phone configuration file must exist on the phone, and the Cisco Unified CME entry and certificate must exist in the file.

File Authentication

The file authentication process validates digitally signed files that a phone downloads from a Trivial File Transfer Protocol (TFTP) server—for example, configuration files, ring list files, locale files, and CTL files. When the phone receives these types of files from the TFTP server, the phone validates the file signatures to verify that file tampering did not occur after the files were created.

Signaling Authentication

The signaling authentication process, also known as signaling integrity, uses the TLS protocol to validate that signaling packets have not been tampered with during transmission. Signaling authentication relies on the creation of the CTL file.

Public Key Infrastructure

Cisco Unified CME phone authentication uses the public-key-infrastructure (PKI) capabilities in Cisco IOS software for certificate-based authentication of IP phones. PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secure data network. Every entity (a person or a device) participating in the secure communication is enrolled in the PKI using a process in which the entity generates a Rivest-Shamir-Adleman (RSA) key pair (one private key and one public key) and has its identity validated by a trusted entity (also known as a certification authority [CA] or trustpoint).

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a CA.

When peers must negotiate a secure communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

Phone Authentication Components

A variety of components work together to ensure secure communications in a Cisco Unified CME system. Table 39: Cisco Unified CME Phone Authentication Components , on page 584 describes the Cisco Unified CME phone authentication components.

Table 39: Cisco Unified CME Phone Authentication Components

Component	Definition
certificate	An electronic document that binds a user's or device's name to its public key. Certificates are commonly used to validate digital signatures. Certificates are needed for authentication during secure communication. An entity obtains a certificate by enrolling with the CA.
signature	An assurance from an entity that the transaction it accompanies is authentic. The entity’s private key is used to sign transactions and the corresponding public key is used for decryption.

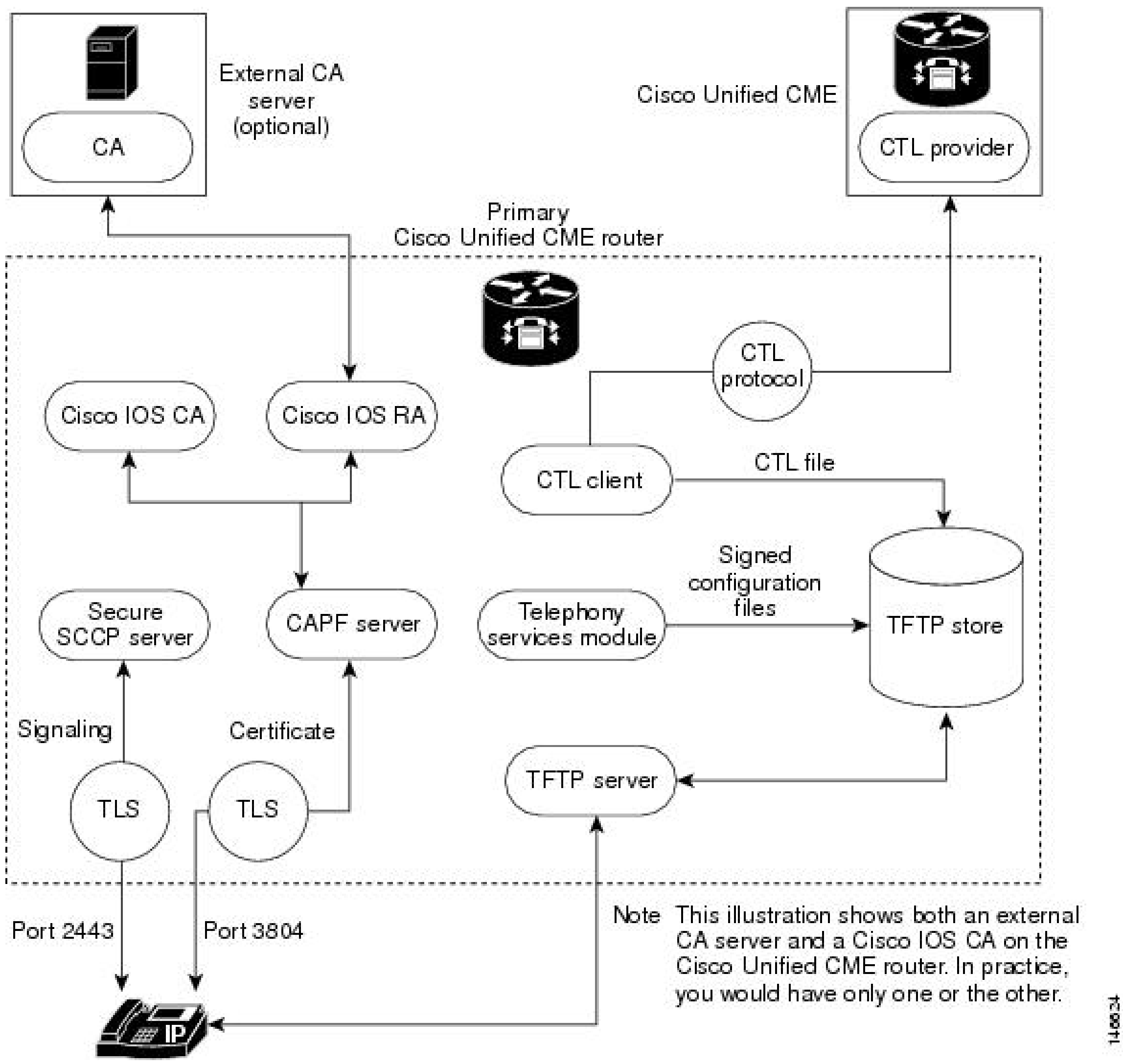
Component	Definition
RSA key pair	RSA is a public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. An RSA key pair consists of a public key and a private key. The public key is included in a certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers. You can configure multiple RSA key pairs to match policy requirements, such as key length, key lifetime, and type of keys, for different certificate authorities or for different certificates.
certificate server trustpoint	A certificate server generates and issues certificates on receipt of legitimate requests. A trustpoint with the same name as the certificate server stores the certificates. Each trustpoint has one certificate plus a copy of the CA certificate.
certification authority (CA)	The root certificate server. It is responsible for managing certificate requests and issuing certificates to participating network devices. This service provides centralized key management for participating devices and is explicitly trusted by the receiver to validate identities and to create digital certificates. The CA can be a Cisco IOS CA on the Cisco Unified CME router, a Cisco IOS CA on another router, or a third-party CA.
registration authority (RA)	Records or verifies some or all of the data required for the CA to issue certificates. It is required when the CA is a third-party CA or Cisco IOS CA is not on the Cisco Unified CME router.

Component	Definition
certificate trust list (CTL) file CTL client CTL provider	A mandatory structure that contains the public key information (server identities) of all the servers with which the IP phone needs to interact (for example, the Cisco Unified CME server, TFTP server, and CAPF server). The CTL file is digitally signed by the SAST. After you configure the CTL client, it creates the CTL file and makes it available in the TFTP directory. The CTL file is signed using the SAST certificate's corresponding private key. An IP phone is then able to download this CTL file from the TFTP directory. The filename format for each phone's CTL file is CTLSEP<mac-addr>.tlv. When the CTL client is run on a router in the network that is not a Cisco Unified CME router, you must configure a CTL provider on each Cisco Unified CME router in the network. Similarly, if a CTL client is running on one of two Cisco Unified CME routers in a network, a CTL provider must be configured on the other Cisco Unified CME router. The CTL protocol transfers information to and from the CTL provider that allows the second Cisco Unified CME router to be trusted by phones and vice versa.
certificate revocation list (CRL)	File that contains certificate expiration dates and used to determine whether a certificate that is presented is valid or revoked.
system administrator security token (SAST)	Part of the CTL client that is responsible for signing the CTL file. The Cisco Unified CME certificate and its associated key pair are used for the SAST function. There are actually two SAST records pertaining to two different certificates in the CTL file for security reasons. They are known as SAST1 and SAST2. If one of the certificates is lost or compromised, then the CTL client regenerates the CTL file using the other certificate. When a phone downloads the new CTL file, it verifies with only one of the two original public keys that was installed earlier. This mechanism is to prevent IP phones from accepting CTL files from unknown sources.

Component	Definition
certificate authority proxy function (CAPF)	Entity that issues certificates (LSCs) to phones that request them. The CAPF is a proxy for the phones, which are unable to directly communicate with the CA. The CAPF can also perform the following certificate-management tasks: • Upgrade existing locally significant certificates on the phones. • Retrieve phone certificates for viewing and troubleshooting. • Delete LSCs on the phone.
manufacture-installed certificate (MIC) locally significant certificate (LSC)	Phones need certificates to engage in secure communications. Many phones come from the factory with MICs, but MICs may expire or become lost or compromised. Some phones do not come with MICs. LSCs are certificates that are issued locally to the phones using the CAPF server.
transport Layer Security (TLS) protocol	IETF standard (RFC 2246) protocol, based on Netscape Secure Socket Layer (SSL) protocol. TLS sessions are established using a handshake protocol to provide privacy and data integrity. The TLS record layer fragments and defragments, compresses and decompresses, and performs encryption and decryption of application data and other TLS information, including handshake messages.

Figure 20: Cisco Unified CME Phone Authentication, on page 588 shows the components in a Cisco Unified CME phone authentication environment.

Figure 20: Cisco Unified CME Phone Authentication



Phone Authentication Process

The following is a high-level summary of the phone-authentication process.

To enable Cisco Unified CME phone authentication:

1 Certificates are issued.

   The CA issues certificates to Cisco Unified CME, SAST, CAPF, and TFTP functions.

2 The CTL file is created, signed and published.

a. The CTL file is created by the CTL client, which is configuration driven. Its goal is to create a CTLfile.tlv for each phone and deposit it in the TFTP directory. To complete its task, the CTL client needs the certificates and public key information of the CAPF server, Cisco Unified CME server, TFTP server, and SASTs.

b. The CTL file is signed by the SAST credentials. There are two SAST records pertaining to two different certificates in the CTL file for security reasons. If one of the certificates is lost or compromised, then the CTL client regenerates the CTL file using the other certificate. When a phone downloads the new CTL file, it verifies the download with only one of the two original public keys that was installed earlier. This mechanism prevents IP phones from accepting CTL files from unknown sources.

c. The CTL file is published on the TFTP server. Because an external TFTP server is not supported in secure mode, the configuration files are generated by the Cisco Unified CME system itself and are digitally signed by the TFTP server's credentials. The TFTP server credentials can be the same as the Cisco Unified CME credentials. If desired, a separate certificate can be generated for the TFTP function if the appropriate trustpoint is configured under the CTL-client interface.

3. The telephony service module signs phone configuration files and each phone requests its file.

4. When an IP phone boots up, it requests the CTL file (CTLfile.tlv) from the TFTP server and downloads its digitally signed configuration file, which has the filename format of SEP<mac-address>.cnf.xml.sgn.

5. The phone then reads the CAPF configuration status from the configuration file. If a certificate operation is needed, the phone initiates a TLS session with the CAPF server on TCP port 3804 and begins the CAPF protocol dialogue. The certificate operation can be an upgrade, delete, or fetch operation. If an upgrade operation is needed, the CAPF server makes a request on behalf of the phone for a certificate from the CA. The CAPF server uses the CAPF protocol to obtain the information it needs from the phone, such as the public key and phone ID. After the phone successfully receives a certificate from the server, the phone stores it in its flash memory.

6. With the certificate in its flash, the phone initiates a TLS connection with the secure Cisco Unified CME server on a well-known TCP port (2443) if the device security mode settings in the .cnf.xml file are set to authenticated or encrypted. This TLS session is mutually authenticated by both parties. The IP phone knows the Cisco Unified CME server's certificate from the CTL file, which it initially downloaded from the TFTP server. The phone's LSC is a trusted party for the Cisco Unified CME server because the issuing CA certificate is present in the router.

Startup Messages

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 that show a temporary inability to configure the certificate server because the startup configuration has not been fully parsed yet. The messages are useful for debugging if the startup configuration has been corrupted.

Configuration File Maintenance

In a secure environment, several types of configuration files must be digitally signed before they can be hosted and used. The filenames of all signed files have a .sgn suffix.

The Cisco Unified CME telephony service module creates phone configuration files (.cnf.xml suffix) and hosts them on a Cisco IOS TFTP server. These files are signed by the TFTP server's credentials.

In addition to the phone configuration files, other Cisco Unified CME configuration files such as the network and user-locale files must be signed. These files are internally generated by Cisco Unified CME, and the signed versions are automatically created in the current code path whenever the unsigned versions are updated or created.

Other configuration files that are not generated by Cisco Unified CME, such as ringlist.xml, distinctiveringlist.xml, audio files, and so forth, are often used for Cisco Unified CME features. Signed versions of these configuration files are not automatically created. Whenever a new configuration file that has not been generated by Cisco Unified CME is imported into Cisco Unified CME, use the **load-cfg-file** command, which does all of the following:

- Hosts the unsigned version of the file on the TFTP server.
- Creates a signed version of the file.
- Hosts the signed version of the file on the TFTP server.

You can also use the **load-cfg-file** command instead of the **tftp-server** command when only the unsigned version of a file needs to be hosted on the TFTP server.

CTL File Maintenance

The CTL file contains the SAST records and other records. (A maximum of two SAST records may exist.) The CTL file is digitally signed by one of the SAST credentials that are listed in the CTL file before the CTL file is downloaded by the phone and saved in its flash. After receiving the CTL file, a phone trusts a newer or changed CTL file only if it is signed by one of the SAST credentials that is present in the original CTL file.

For this reason, you should take care to regenerate the CTL file only with one of the original SAST credentials. If both SAST credentials are compromised and a CTL file must be generated with a new credential, you must reset the phone to its factory defaults.

CTL Client and Provider

The CTL client generates the CTL file. The CTL client must be provided with the names of the trustpoints it needs for the CTL file. It can run on the same router as Cisco Unified CME or on another, standalone router. When the CTL client runs on a standalone router (not a Cisco Unified CME router), you must configure a CTL provider on each Cisco Unified CME router. The CTL provider securely communicates the credentials of the Cisco Unified CME server functions to the CTL client that is running on another router.

When the CTL client is running on either a primary or secondary Cisco Unified CME router, you must configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running.

The CTL protocol is used to communicate between the CTL client and a CTL provider. Using the CTL protocol ensures that the credentials of all Cisco Unified CME routers are present in the CTL file and that all

Cisco Unified CME routers have access to the phone certificates that were issued by the CA. Both elements are prerequisites to secure communications.

To enable CTL clients and providers, see Configure the CTL Client, on page 607 and Configure the CTL Provider, on page 619.

Manually Importing MIC Root Certificate

When a phone uses a MIC for authentication during the TLS handshake with the CAPF server, the CAPF server must have a copy of the MIC to verify it. Different certificates are used for different types of IP phones.

A phone uses a MIC for authentication when it has a MIC but no LSC. For example, you have a Cisco Unified IP Phone 7970 that has a MIC by default but no LSC. When you schedule a certificate upgrade with the authentication mode set to MIC for this phone, the phone presents its MIC to the Cisco Unified CME CAPF server for authentication. The CAPF server must have a copy of the MIC's root certificate to verify the phone's MIC. Without this copy, the CAPF upgrade operation fails.

To ensure that the CAPF server has copies of the MICs it needs, you must manually import certificates to the CAPF server. The number of certificates that you must import depends on your network configuration. Manual enrollment refers to copy-and-paste or TFTP transfer methods.

To manually import the MIC root certificate, see Manually Import the MIC Root Certificate, on page 626.

Feature Design of Media Encryption

Companion voice security Cisco IOS features provide an overall architecture for secure end-to-end IP telephony calls on supported network devices that enable the following:

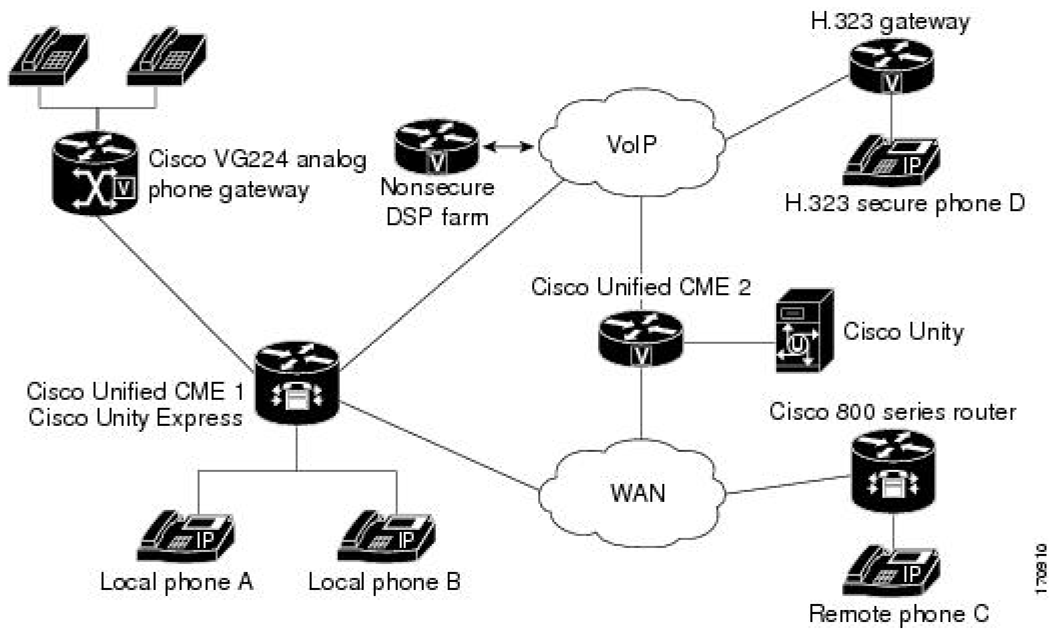
- SRTP-capable Cisco Unified CME networks with secure interoperability
- Secure Cisco IP phone calls
- Secure Cisco VG224 Analog Phone Gateway endpoints
- Secure supplementary services

These features are implemented using media and signaling authentication and encryption in Cisco IOS H.323 networks. H.323, the ITU-T standard that describes packet-based video, audio, and data conferencing, refers to a set of other standards, including H.450, to describe its actual protocols. H.323 allows dissimilar communication devices to communicate with each other by using a standard communication protocol and defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods. H.450, a component of the H.323 standard, defines signaling and procedures that are used to provide telephony-like supplementary services. H.450 messages are used in H.323 networks to implement secure supplementary service support and also empty capability set (ECS) messaging for media capability negotiation.

Secure Cisco Unified CME

The secure Cisco Unified CME solution includes secure-capable voice ports, SCCP endpoints, and a secure H.323 trunk between Cisco Unified CME and Cisco Unified Communications Manager for audio media. SIP trunks are not supported. Figure 21: Secure Cisco Unified CME System, on page 592 shows the components of a secure Cisco Unified CME system.

Figure 21: Secure Cisco Unified CME System



Secure Cisco Unified CME implements call control signaling using Transport Layer Security (TLS) or IPsec (IP Security) for the secure channel and uses SRTP for media encryption. Secure Cisco Unified CME manages the SRTP keys to endpoints and gateways.

The Media Encryption (SRTP) on Cisco Unified CME feature supports the following features:

- SCCP endpoints.
- Secure voice calls in a mixed shared line environment that allows both RTP- and SRTP-capable endpoints; shared line media security depends on the endpoint configuration.
- Secure supplementary services using H.450 including:
  - Call forward
  - Call transfer
  - Call hold and resume
  - Call park and call pickup
  - Nonsecure software conference

Note SRTP conference calls over H.323 may experience a zero- to two-second noise interval when the call is joined to the conference.

- Secure calls in a non-H.450 environment.

- Secure Cisco Unified CME interaction with secure Cisco Unity.
- Secure Cisco Unified CME interaction with Cisco Unity Express (interaction is supported and calls are downgraded to nonsecure mode).
- Secure transcoding for remote phones with DSP Farm transcoding configured.

These features are discussed in the following sections.

Secure Supplementary Services

The Media Encryption (SRTP) feature supports secure supplementary services in both H.450 and non-H.450 Cisco Unified CME networks. A secure Cisco Unified CME network should be either H.450 or non-H.450, not a hybrid.

Secure SIP Trunk Support on Cisco Unified CME

Prior to Cisco Unified CME Relese 10 release, supplementary services were not supported on the secure SIP trunk of the secure SCCP Cisco Unified CME. This feature supports the following supplementary services in the secure SRTP and SRTP fallback modes on the SIP trunk of the SCCP Cisco Unified CME:

- Basic secure calls
- Call hold and resume
- Call transfer (blind and consult)
- Call forward (CFA,CFB,CFNA)
- DTMF support
- Call park and pickup
- Voice mail systems using CUE (works only with SRTP fallback mode)

To enable the supplementary services, use the existing "**supplementary-service media-renegotiate**" command as shown in the following example:

```
(config)# voice service voip
(conf-voi-serv)# no ip address trusted authenticate
(conf-voi-serv)# srtp
(conf-voi-serv)# allow-connections sip to sip
(conf-voi-serv)# no supplementary-service sip refer
(conf-voi-serv)# supplementary-service media-renegotiate
```

Note In the SRTP mode, nonsecure media (RTP) format is not allowed across the secure SIP trunk. For Music On Hold, Tone On Hold, and Ring Back Tone, the tone is not played across the SIP trunk. In SRTP fallback mode, media across the secure SIP trunk is switched over to RTP if the remote end is nonsecure or while playing the MMusic On Hold, Tone On Hold, and Ring Back Tone.

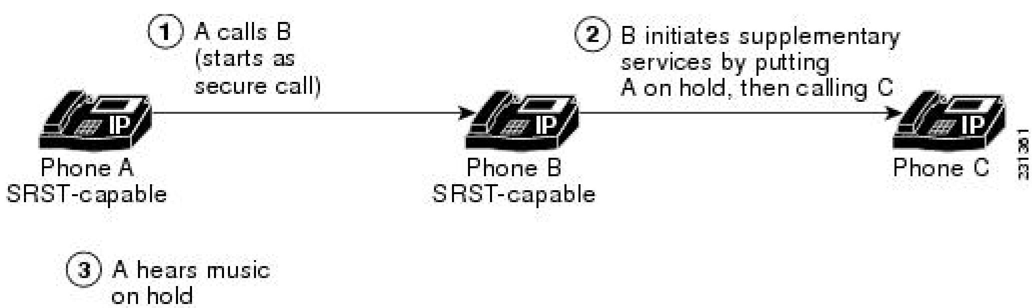
Restriction

- Secure SIP trunk is supported only on SCCP Cisco Unified CME and not on SIP Cisco Unified CME. Secure SIP lines are not supported on the Cisco Unified CME mode.
- Xcoder support is not available for playing secure tones (Music On Hold, Tone On Hold, and Ring Back Tone).
- Tones are not played in the SRTP mode because these tones are available only in non-secure (RTP) format.
- We recommend that you configure **no supplementary-service sip refer** command for SCCP Cisco Unfied CME for the supplementary services.

Secure Cisco Unified CME in an H.450 Environment

Signaling and media encryption among secure endpoints is supported, enabling supplementary services such as call transfer (H.450.2) and call forward (H.450.3) between secure endpoints. Call park and pick up use H.450 messages. Secure Cisco Unified CME is H.450-enabled by default; however, secure music on hold (MOH) and secure conferences (three-way calling) are not supported. For example, when supplementary services are initiated as shown in Figure 22: Music on Hold in an H.450 Environment, on page 594, ECS and Terminal Capabilities Set (TCS) are used to negotiate the initially secure call between A and B down to RTP so A can hear MOH. When B resumes the call to A, the call goes back to SRTP. Similarly, when a transfer is initiated, the party being transferred is put on hold and the call is negotiated down to RTP. When the call is transferred, it goes back to SRTP if the other end is SRTP capable.

Figure 22: Music on Hold in an H.450 Environment



Secure Cisco Unified CME in a Non H.450 Environment

Security for supplementary services requires midcall key negotiation or midcall media renegotiation. In an H.323 network where there are no H.450 messages, media renegotiation is implemented using ECS for scenarios such as mismatched codecs and secure calls. If you disable H.450 on the router globally, the configuration is applied to RTP and SRTP calls. The signaling path is hairpin on XOR for Cisco Unified CME and Cisco Unified Communications Manager. For example, in Figure 23: Transfer in a Non-H.450 Environment, on page 595, the signaling path goes from A through B (the supplementary services initiator) to C. When deploying voice security in this scenario, consider that the media security keys will pass through

XOR, that is, through B, the endpoint that issued the transfer request. To avoid the man-in-the-middle attack, the XOR must be a trusted entity.

Figure 23: Transfer in a Non-H.450 Environment

The media path is optional. The default media path for Cisco Unified CME is hairpin. However, whenever possible media flow around can be configured on Cisco Unified CME. When configuring media flow through, which is the default, remember that chaining multiple XOR gateways in the media path introduces more delay and thus reduces voice quality. Router resources and voice quality limit the number of XOR gateways that can be chained. The requirement is platform dependent and may vary between signaling and media. The practical chaining level is three.

A transcoder is inserted when there is a codec mismatch and ECS and TCS negotiation fails. For example, if Phone A and Phone B are SRTP capable, but Phone A uses the G.711 codec and Phone B uses the G.729 codec, a transcoder is inserted if Phone B has one. However, the call is negotiated down to RTP to fulfill the codec requirement so the call is not secure.

Secure Transcoding for Remote Phones with DSP Farm Transcoding Configured

Transcoding is supported for remote phones that have the **dspfarm-assist** keyword of the **codec** command configured. A remote phone is a phone that is registered to a Cisco Unified CME and is residing on a remote location across the WAN. To save bandwidth across the WAN connection, calls to such a phone can be made to use the G.729r8 codec by configuring the **codec g729r8 dspfarm assist** command for the ephone. The **g729r8** keyword forces calls to such a phone to use the G.729 codec. The **dspfarm-assist** keyword enables using available DSP resources if an H.323 call to the phone needs to be transcoded.

Note Transcoding is enabled only if an H.323 call with a different codec from the remote phone tries to make a call to the remote phone. If a local phone on the same Cisco Unified CME as the remote phone makes a call to the remote phone, the local phone is forced to change its codec to G.729 instead of using transcoding.

Secure transcoding for point-to-point SRTP calls can only occur when both the SCCP phone that is to be serviced by Cisco Unified CME transcoding and its peer in the call are SRTP capable and have successfully negotiated the SRTP keys. Secure transcoding for point-to-point SRTP calls cannot occur when only one of the peers in the call is SRTP capable.

If Cisco Unified CME transcoding is to be performed on a secure call, the Media Encryption (SRTP) on Cisco Unified CME feature allows Cisco Unified CME to provide the DSP Farm with the encryption keys for the secure call as additional parameters so that Cisco Unified CME transcoding can be performed successfully. Without the encryption keys, the DSP Farm would not be able to read the encrypted voice data to transcode it.

Note The secure transcoding described here does not apply to IP-IP gateway transcoding.

Cisco Unified CME transcoding is different from IP-to-IP gateway transcoding because it is invoked for an SCCP endpoint only, instead of for bridging VoIP call legs. Cisco Unified CME transcoding and IP-to-IP gateway transcoding are mutually exclusive, that is, only one type of transcoding can be invoked for a call. If no DSP Farm capable of SRTP transcoding is available, Cisco Unified CME secure transcoding is not performed and the call goes through using G.711.

For configuration information, see Register the DSP Farm with Cisco Unified CME 4.2 or a Later Version in Secure Mode, on page 496.

Secure Cisco Unified CME with Cisco Unity Express

Cisco Unity Express does not support secure signaling and media encryption. Secure Cisco Unified CME interoperates with Cisco Unity Express but calls between Cisco Unified CME and Cisco Unity Express are not secure.

In a typical Cisco Unity Express deployment with Cisco Unified CME in a secure H.323 network, Session Initiation Protocol (SIP) is used for signaling and the media path is G.711 with RTP. For Call Forward No Answer (CFNA) and Call Forward All (CFA), before the media path is established, signaling messages are sent to negotiate an RTP media path. If codec negotiation fails, a transcoder is inserted. The Media Encryption (SRTP) on Cisco Unified CME feature's H.323 service provider interface (SPI) supports fast start calls. In general, calls transferred or forwarded back to Cisco Unified CME from Cisco Unity Express fall into existing call flows and are treated as regular SIP and RTP calls.

The Media Encryption (SRTP) on Cisco Unified CME feature supports blind transfer back to Cisco Unified CME only. When midcall media renegotiation is configured, the secure capability for the endpoint is renegotiated regardless of which transfer mechanism, H.450.2 or Empty Capability Set (ECS), is used.

Secure Cisco Unified CME with Cisco Unity

The Media Encryption (SRTP) on Cisco Unified CME feature supports Cisco Unity 4.2 or a later version and Cisco Unity Connection 1.1 or a later version using SCCP. Secure Cisco Unity for Cisco Unified CME acts like a secure SCCP phone. Some provisioning is required before secure signaling can be established. Cisco Unity receives Cisco Unified CME device certificates from the Certificate Trust List (CTL) and Cisco Unity certificates are inserted into Cisco Unified CME manually. Cisco Unity with SIP is not supported.

The certificate for the Cisco Unity Connection is in the Cisco Unity administration web application under the "port group settings."

HTTPS Provisioning For Cisco Unified IP Phones

This section contains the following topics:

- HTTPS support for an External Server, on page 597
- HTTPS Support in Cisco Unified CME, on page 597

HTTPS support for an External Server

There is an increasing need to securely access web content on Cisco Unified IP phones using HTTPS. The X.509 certificate of a third-party web server must be stored in the IP phone's CTL file to authenticate the web server but the **server** command used to enter trustpoint information cannot be used to import the certificate to the CTL file. Because the **server** command requires the private key from the third-party web server for certificate chain validation and you cannot obtain that private key from the web server, the **import certificate** command is added to save the trusted certificate in the CTL file.

For information on how to import a trusted certificate to an IP phone's CTL file for HTTPS provisioning, see HTTPS Provisioning for Cisco Unified IP Phones, on page 637.

For information on phone authentication support in Cisco Unified CME, see Phone Authentication Overview, on page 582.

HTTPS Support in Cisco Unified CME

Cisco Unified IP phones use HTTP for some of the services offered by Cisco Unified CME. These services, which include local-directory lookup on Cisco Unified CME, My Phone Apps, and Extension Mobility, are invoked by pressing the "Services" button on the phones.

With Hypertext Transfer Protocol Secure (HTTPS) support in Cisco Unified CME 9.5 and later versions, these services can be invoked using an HTTPS connection from the phones to Cisco Unified CME.

Note Ensure that the configured phone is provisioned for HTTPS-based services that run on Cisco Unified CME before configuring HTTPS globally or locally. Please refer to the appropriate phone administrator guide to know if your Cisco Unified IP phone supports HTTPS access. HTTP services continue to run for other phones that do not support HTTPS.

For information on provisioning Cisco Unified IP phones for secure access to web content using HTTPS, see HTTPS Provisioning for Cisco Unified IP Phones, on page 637.

For configuration examples, see Example for Configuring HTTPS Support for Cisco Unified CME, on page 655.

Configure Security

Configure the Cisco IOS Certification Authority

To configure a Cisco IOS Certification Authority (CA) on a local or external router, perform the following steps.

Note If you use a third-party CA, follow the provider's instructions instead of performing these steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *label*
5. **database level** {**minimal** | **names** | **complete**}
6. **database url** *root-url*
7. **lifetime certificate** *time*
8. **issuer-name CN=***label*
9. **exit**
10. **crypto pki trustpoint** *label*
11. **enrollment url** *ca-url*
12. **exit**
13. **crypto pki server** *label*
14. **grant auto**
15. **no shutdown**
16. **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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the Cisco web-browser user interface on the local Cisco Unified CME router.
Step 4	**crypto pki server** *label* **Example:** `Router(config)# crypto pki server sanjose1`	Defines a label for the Cisco IOS CA and enters certificate-server configuration mode.
Step 5	**database level** {**minimal** | **names** | **complete**}	(Optional) Controls the type of data stored in the certificate enrollment database.

	Command or Action	Purpose
	Example: `Router(config-cs-server)# database level complete`	• **minimal**—Enough information is stored only to continue issuing new certificates without conflict. This is the default value. • **names**—In addition to the minimal information given, the serial number and subject name of each certificate are also provided. • **complete**—In addition to the information given in the minimal and names levels, each issued certificate is written to the database. If you use this keyword, you must also specify an external TFTP server in which to store the data by using the **database url** command.
Step 6	**database url** *root-url* **Example:** `Router(config-cs-server)# database url nvram:`	(Optional) Specifies the location, other than NVRAM, where all database entries for the certificate server are to be written out. • Required if you configured the **complete** keyword with the **database level** command in the previous step. • *root-url*—URL that is supported by the Cisco IOS file system and where database entries are to be written out. If the CA is going to issue a large number of certificates, select an appropriate storage location like flash or other storage device to store the certificates. • When the storage location chosen is flash and the file system type on this device is Class B (LEFS), make sure to check free space on the device periodically and use the **squeeze** command to free the space used up by deleted files. This process may take several minutes and should be done during scheduled maintenance periods or off-peak hours.
Step 7	**lifetime certificate** *time* **Example:** `Router(config-cs-server) lifetime certificate 888`	(Optional) Specifies the lifetime, in days, of certificates issued by this Cisco IOS CA. • *time*—Number of days until a certificate expires. Range is 1 to 1825 days. Default is 365. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate. • Configure this command before the Cisco IOS CA is enabled by using the **no shutdown** command.
Step 8	**issuer-name CN=***label* **Example:** `Router(config-cs-server)# issuer-name CN=sanjose1`	(Optional) Specifies a distinguished name (DN) as issuer name for the Cisco IOS CA. • Default is already-configured label for the Cisco IOS CA. See Step 4, on page 598.
Step 9	**exit** **Example:** `Router(config-cs-server)# exit`	Exits certificate-server configuration mode.
Step 10	**crypto pki trustpoint** *label*	(Optional) Declares a trustpoint and enters ca-trustpoint configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# crypto pki trustpoint sanjose1`	• For local CA only. This command is not required for Cisco IOS CA on an external router. • If you must use a specific RSA key for the Cisco IOS CA, use this command to create your own trustpoint by using the same label to be used with the **crypto pki server** command. If the router sees a configured trustpoint with the same label as the crypto pki server, it uses this trustpoint and does not automatically create a trustpoint.
Step 11	**enrollment url** *ca-url* **Example:** `Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com`	Specifies the enrollment URL of the issuing Cisco IOS CA. • For local Cisco IOS CA only. This command is not required for Cisco IOS CA on an external router. • *ca-url*—URL of the router on which the Cisco IOS CA is installed.
Step 12	**exit** **Example:** `Router(config-ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.
Step 13	**crypto pki server** *label* **Example:** `Router(config)# crypto pki server sanjose1`	Enters certificate-server configuration mode. • *label*—Name of the Cisco IOS CA being configured.
Step 14	**grant auto** **Example:** `Router(config-cs-server)# grant auto`	(Optional) Allows certificates to be issued automatically to any requester. • Default and recommended method is manual enrollment. • Use this command only when testing and building simple networks. Use the **no grant auto** command after configuration is complete to prevent certificates from being automatically granted.
Step 15	**no shutdown** **Example:** `Router(config-cs-server)# no shutdown`	(Optional) Enables the Cisco IOS CA. • Use this command only after you are finished configuring the Cisco IOS CA.
Step 16	**end** **Example:** `Router(config-cs-server)# end`	Returns to privileged EXEC mode.

The following partial output from the **show running-config** command shows the configuration for a Cisco IOS CA named sanjose1 running on the local Cisco Unified CME router:

```
ip http server

crypto pki server sanjose1
 database level complete
 database url nvram:

crypto pki trustpoint sanjose1
 enrollment url http://ca-server.company.com

crypto pki server authority1
 no grant auto
 no shutdown
```

Obtain Certificates for Server Functions

The CA issues certificates for the following server functions:

- Cisco Unified CME—Requires a certificate for TLS sessions with phones.
- TFTP—Requires a key pair and certificate for signing configuration files.
- HTTPS—Requires a key pair and certificate for signing configuration files.
- CAPF—Requires a certificate for TLS sessions with phones.
- SAST—Required for signing the CTL file. We recommend creating two SAST certificates, one for primary use and one for backup.

To obtain a certificate for a server function, perform the following steps for each server function.

Note You can configure a different trustpoint for each server function or you can configure the same trustpoint for more than one server function as shown in Configuration Examples for Security, on page 643 at the end of this module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *trustpoint-label*
4. **enrollment url** *url*
5. **revocation-check** *method1* [*method2* [*method3*]]
6. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
7. **exit**
8. **crypto pki authenticate** *trustpoint-label*
9. **crypto pki enroll** *trustpoint-label*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *trustpoint-label* **Example:** `Router(config)# crypto pki trustpoint capf`	Declares the trustpoint that the CA should use and enters ca-trustpoint configuration mode. • *trustpoint-label*—Label for server function being configured.
Step 4	**enrollment url** *url* **Example:** `Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com`	Specifies the enrollment URL of the issuing CA. • *url*—URL of the router on which the issuing CA is installed.
Step 5	**revocation-check** *method1* [*method2* [*method3*]] **Example:** `Router(config-ca-trustpoint)# revocation-check none`	(Optional) Specifies the method to be used to check the revocation status of a certificate. • *method*—If a second and third method are specified, each subsequent method is used only if the previous method returns an error, such as a server being down. • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an Online Certificate Status Protocol (OCSP) server.
Step 6	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(config-ca-trustpoint)# rsakeypair capf 1024 1024`	(Optional) Specifies a key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured. • *key-size*—Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—Size of the second key, which is used to request separate encryption, signature keys, and certificates. • Multiple trustpoints can share the same key.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.
Step 8	**crypto pki authenticate** *trustpoint-label* **Example:** `Router(config)# crypto pki authenticate capf`	Retrieves the CA certificate, authenticates it, and checks the certificate fingerprint if prompted. • This command is optional if the CA certificate is already loaded into the configuration • *trustpoint-label*—Already-configured label for server function being configured.
Step 9	**crypto pki enroll** *trustpoint-label* **Example:** **crypto pki enroll** `trustpoint-label` `Router(config)# crypto pki enroll capf`	Enrolls with the CA and obtains the certificate for this trustpoint. • *trustpoint-label*—Already-configured label for server function being configured.
Step 10	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

The following partial output from the **show running-config** command show how to obtain certificates for a variety of server functions:

Obtaining a certificate for the CAPF server function

```
!configuring a trust point
 crypto pki trustpoint capf-server
 enrollment url http://192.168.1.1:80
 revocation-check none
!authenticate w/ the CA and download its certificate
crypto pki authenticate capf-server
! enroll with the CA and obtain this trustpoint's certificate
 crypto pki enroll capf-server
```

Obtaining a certificate for the Cisco Unified CME server function

```
crypto pki trustpoint cme-server
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate cme-server
crypto pki enroll cme-server
```

Obtaining a certificate for the TFTP server function

```
crypto pki trustpoint tftp-server
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate tftp-server
crypto pki enroll tftp-server
```

Obtaining a certificate for the first SAST server function (sast1)

```
crypto pki trustpoint sast1
  enrollment url http://192.168.1.1:80
 revocation-check none

 crypto pki authenticate sast1
crypto pki enroll sast1
```

Obtaining a certificate for the second SAST server function (sast2)

```
crypto pki trustpoint sast2
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate sast2
crypto pki enroll sast2
```

Configure Telephony-Service Security Parameters

To configure security parameters for telephony service, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **secure-signaling trustpoint** *label*
5. **tftp-server-credentials trustpoint** *label*
6. **device-security-mode** {**authenticated** | **none** | **encrypted**}
7. **cnf-file perphone**
8. **load-cfg-file** *file-url* **alias** *file-alias* [**sign**] [**create**]
9. **server-security-mode** {**erase** | **non-secure** | **secure**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**secure-signaling trustpoint** *label* **Example:** `Router(config-telephony)# secure-signaling trustpoint cme-sccp`	Configures trustpoint to be used for secure signalling. • *label*—Name of a configured PKI trustpoint with a valid certificate to be used for TLS handshakes with IP phones on TCP port 2443.
Step 5	**tftp-server-credentials trustpoint** *label* **Example:** `Router(config-telephony)# tftp-server-credentials trustpoint cme-tftp`	Configures the TFTP server credentials (trustpoint) to be used for signing the configuration files. • *label*—Name of a configured PKI trustpoint with a valid certificate to be used to sign the phone configuration files. This can be the CAPF trustpoint that was used in the previous step or any trustpoint with a valid certificate
Step 6	**device-security-mode** {**authenticated** | **none** | **encrypted**} **Example:** `Router(config-telephony)# device-security-mode authenticated`	Enables security mode for endpoints. • **authenticated**—Instructs device to establish a TLS connection with no encryption. There is no Secure Real-Time Transport Protocol (SRTP) in the media path. • **none**—SCCP signaling is not secure. This is the default. • **encrypted**—Instructs device to establish an encrypted TLS connection to secure media path using SRTP. • This command can also be configured in ephone configuration mode. The value set in ephone configuration mode has priority over the value set in telephony-service configuration mode.
Step 7	**cnf-file perphone** **Example:** `Router(config-telephony)# cnf-file perphone`	Specifies that the system generate a separate XML configuration file for each IP phone. • Separate configuration files for each endpoint are required for security.

	Command or Action	Purpose
Step 8	**load-cfg-file** *file-url* **alias** *file-alias* [**sign**] [**create**] **Example:** `Router(config-telephony)# load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign create`	(Optional) Signs configuration files that are not created by Cisco Unified CME. Also loads the signed and unsigned versions of a file on the TFTP server. • *file-url*—Complete path of a configuration file in a local directory. • **alias** *file-alias*—Alias name of the file to be served on the TFTP server. • **sign**—(Optional) The file needs to be digitally signed and served on the TFTP server. • **create**—(Optional) Creates the signed file in the local directory. • The first time that you use this command for each file, use the **create** and **sign** keywords. The **create** keyword is not maintained in the running configuration to prevent signed files from being recreated during every reload. • To serve an already-signed file on the TFTP server, use this command without the **create** and **sign** keywords.
Step 9	**server-security-mode** {**erase** | **non-secure** | **secure**} **Example:** `Router(config-telephony)# server-security-mode non-secure`	(Optional) Changes the security mode of the server. • **erase**—Deletes the CTL file. • **non-secure**—Nonsecure mode. • **secure**—Secure mode. • This command has no impact until the CTL file is initially generated by the CTL client. When the CTL file is generated, the CTL client automatically sets server security mode to secure.
Step 10	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verify Telephony-Service Security Parameters

Step 1 **show telephony-service security-info**

Use this command to display the security-related information that is configured in telephony-service configuration mode.

Example:

`Router#` **show telephony-service security-info**

```
Skinny Server Trustpoint for TLS: cme-sccp
TFTP Credentials Trustpoint: cme-tftp
Server Security Mode: Secure
Global Device Security Mode: Authenticated
```

Step 2 **show running-config**

Use this command to display the running configuration to verify telephony and per-phone security configuration.

Example:

```
Router# show running-config

telephony-service
  secure-signaling trustpoint cme-sccp
  server-security-mode secure
  device-security-mode authenticated
  tftp-server-credentials trustpoint cme-tftp
  .
  .
  .
```

Configure the CTL Client

Perform one of the following tasks, depending upon your network configuration:

- Configure the CTL Client on a Cisco Unified CME Router, on page 607
- Configure the CTL Client on a Router That is Not a Cisco Unified CME Router, on page 610

Configure the CTL Client on a Cisco Unified CME Router

To configure a CTL client for creating a list of known, trusted certificates and tokens on a local Cisco Unified CME router, perform the following steps.

> **Note** If you have primary and secondary Cisco Unified CME routers, you can configure the CTL client on either one of them.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ctl-client**
4. **sast1 trustpoint** *label*
5. **sast2 trustpoint** *label*
6. **server** {**capf** | **cme**| **cme-tftp** | **tftp**} *ip-address* **trustpoint** *trustpoint-label*
7. **server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string*
8. **regenerate**
9. **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	**ctl-client** **Example:** `Router(config)# ctl-client`	Enters CTL-client configuration mode.
Step 4	**sast1 trustpoint** *label* **Example:** `Router(config-ctl-client)# sast1 trustpoint sast1tp`	Configures credentials for the primary SAST. • *label*- Name of SAST1 trustpoint. **Note** SAST1 and SAST2 certificates must be different from each other. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to the factory default.
Step 5	**sast2 trustpoint** *label* **Example:** `Router(config-ctl-client)# sast2 trustpoint`	Configures credentials for the secondary SAST. • *label* - name of SAST2 trustpoint. **Note** SAST1 and SAST2 certificates must be different from each other. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to the factory default.

	Command or Action	Purpose
Step 6	**server** {**capf** | **cme**| **cme-tftp** | **tftp**} *ip-address* **trustpoint** *trustpoint-label* **Example:** `Router(config-ctl-client)# server capf 10.2.2.2 trustpoint capftp`	Configures a trustpoint for each server function that is running locally on the Cisco Unified CME router. • *ip-address* - IP address of the Cisco Unified CME router. If there are multiple network interfaces, use the interface address in the local LAN to which the phones are connected. • **trustpoint** *trustpoint-label*- Name of the PKI trustpoint for the server function being configured. • Repeat this command for server each function that is running locally on the Cisco Unified CME router.
Step 7	**server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string* **Example:** `Router(config-ctl-client)# server cme 10.2.2.2 username user3 password 0 38h2KL`	(Optional) Provides information for another Cisco Unified CME router (primary or secondary) in the network. • *ip-address*- IP address of the othe Cisco Unified CME router. • **username** *name-string*- Username that is configured on the CTL provider. • **password**- Defines the way that you want the password to appear in **show** command output and not to the way that you enter the password. ◦ **0**- Not encrypted. ◦ **1**- Encrypted using Message Digest 5 (MD5). • *password-string*- Administrative password of the CTL provider running on the remote Cisco Unified CME router.
Step 8	**regenerate** **Example:** `Router(config-ctl-client)# regenerate`	Creates a new CTLFile.tlv after you make changes to the CTL client configuration.
Step 9	**end** **Example:** `Router(config-ctl-client)# end`	Returns to privileged EXEC mode.

Examples

The following sample output from the **show ctl-client** command displays the trustpoints in the system:

```
Router# show ctl-client

CTL Client Information
-----------------------------
  SAST 1 Certificate Trustpoint: cmeserver
         SAST 1 Certificate Trustpoint: sast2
```

```
List of Trusted Servers in the CTL
       CME      10.1.1.1         cmeserver
       TFTP     10.1.1.1         cmeserver
       CAPF     10.1.1.1         cmeserver
```

What to Do Next

You are finished configuring the CTL client. See Configure the CAPF Server, on page 612.

Configure the CTL Client on a Router That is Not a Cisco Unified CME Router

To configure a CTL client on a stand-alone router that is not a Cisco Unified CME router, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ctl-client**
4. **sast1 trustpoint** *label*
5. **sast2 trustpoint** *label*
6. **server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string*
7. **regenerate**
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	**ctl-client** **Example:** `Router(config)# ctl-client`	Enters ctl-client configuration mode.
Step 4	**sast1 trustpoint** *label* **Example:** `Router(config-ctl-client)# sast1 trustpoint sast1tp`	Configures credentials for the primary SAST. • *label*—Name of SAST1 trustpoint.

	Command or Action	Purpose
		Note SAST1 and SAST2 certificates must be different from each other but either of them may use the same certificate as the Cisco Unified CME router to conserve memory. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to the factory default.
Step 5	**sast2 trustpoint** *label* **Example:** `Router(config-ctl-client)# sast2 trustpoint`	Configures credentials for the secondary SAST. • *label*—name of SAST2 trustpoint. **Note** SAST1 and SAST2 certificates must be different from each other but either of them may use the same certificate as the Cisco Unified CME router to conserve memory. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to the factory default.
Step 6	**server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string* **Example:** `Router(config-ctl-client)# server cme 10.2.2.2 username user3 password 0 38h2KL`	(Optional) Provides information about another Cisco Unified CME router (primary or secondary) in the network, if one exists. • *ip-address*—IP address of the other Cisco Unified CME router. • **username** *name-string*—Username that is configured on the CTL provider. • **password**—Encryption status of the password string. ◦ **0**—Not encrypted. ◦ **1**—Encrypted using Message Digest 5 (MD5). **Note** This option refers to the way that you want the password to appear in show command output and not to the way that you enter the password in this command. • *password-string*—Administrative password of the CTL provider running on the remote Cisco Unified CME router.
Step 7	**regenerate** **Example:** `Router(config-ctl-client)# regenerate`	Creates a new CTLFile.tlv after you make changes to the CTL client configuration.
Step 8	**end** **Example:** `Router(config-ctl-client)# end`	Returns to privileged EXEC mode.

Examples

The following sample output from the **show ctl-client** command displays the trustpoints in the system:

```
Router# show ctl-client

CTL Client Information
-----------------------------
 SAST 1 Certificate Trustpoint: cmeserver
        SAST 1 Certificate Trustpoint: sast2
        List of Trusted Servers in the CTL
                CME     10.1.1.1        cmeserver
                TFTP    10.1.1.1        cmeserver
                CAPF    10.1.1.1        cmeserver
```

Configure the CAPF Server

A certificate must be obtained for the CAPF server so that it can establish a TLS session with the phone during certificate operation. The CAPF server can install, fetch, or delete locally significant certificates (LSCs) on security-enabled phones. To enable the CAPF server on the Cisco Unified CME router, perform the following steps.

Tip When you use the CAPF server to install phone certificates, arrange to do so during a scheduled period of maintenance. Generating many certificates at the same time may cause call-processing interruptions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **capf-server**
4. **trustpoint-label** *label*
5. **cert-enroll-trustpoint** *label* **password** {**0** |**1**} *password-string*
6. **source-addr** *ip-address*
7. **auth-mode** {**auth-string** | **LSC** | **MIC** | **none** | **null-string**}
8. **auth-string** {**delete** | **generate**} {**all** | *ephone-tag*} [*digit-string*]
9. **phone-key-size** {**512** | **1024** | **2048**}
10. **port** *tcp-port*
11. **keygen-retry** *number*
12. **keygen-timeout** *minutes*
13. **cert-oper** {**delete all** | **fetch all** | **upgrade all**}
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**capf-server** **Example:** `Router(config)# capf-server`	Enters capf-server configuration mode.
Step 4	**trustpoint-label** *label* **Example:** `Router(config-capf-server)# trustpoint-label tp1`	Specifies the label for the trustpoint. • *label*—Name of trustpoint whose certificate is to be used for TLS connection between the CAPF server and the phone.
Step 5	**cert-enroll-trustpoint** *label* **password** {**0** |**1**} *password-string* **Example:** `Router(config-capf-server)# cert-enroll-trustpoint ra1 password 0 x8oWiet`	Enrolls the CAPF with the CA (or RA, if the CA is not local to the Cisco Unified CME router). • *label*—PKI trustpoint label for CA and RA that was previously configured by using the **crypto pki trustpoint** command in global configuration mode. • **password—**Encryption status of the password string. • *password-string*—Password to use for certificate enrollment. This password is the revocation password that is sent along with the certificate request to the CA.
Step 6	**source-addr** *ip-address* **Example:** `Router(config-capf-server)# source addr 10.10.10.1`	Defines the IP address of the CAPF server on the Cisco Unified CME router.
Step 7	**auth-mode** {**auth-string** | **LSC** | **MIC** | **none** | **null-string**} **Example:** `Router(config-capf-server)# auth-mode auth-string`	Specifies the type of authentication mode for CAPF sessions to verify endpoints that request certificates. • **auth-string—**The phone user enters a special authentication string at the phone. The string is provided to the user by the system administrator and is configured using the **auth-string generate** command. • **LSC—**The phone provides its LSC for authentication, if one exists. • **MIC—**The phone provides its MIC for authentication, if one exists. If this option is chosen, the MIC s issuer certificate must be imported into a PKI trustpoint.

	Command or Action	Purpose
		• **none**—No certificate upgrade is initiated. This is the default. • **null-string**—No authentication.
Step 8	**auth-string** {**delete** | **generate**} {**all** | *ephone-tag*} [*digit-string*] **Example:** `Router(config-capf-server)# auth-string generate all`	(Optional) Creates or removes authentication strings for one or all secure phones. • Use this command if the **auth-string** keyword is specified in the previous step. Strings become part of the ephone configuration. • **delete**—Remove authentication strings for the specified secure devices. • **generate**—Create authentication strings for the specified secure devices. • **all**—All phones. • *ephone-tag*—identifier for the ephone to receive the authentication string. • *digit-string*—Digits that phone user must dial for CAPF authentication. Length of string is 4 to 10 digits that can be pressed on the keypad. If this value is not specified, a random string is generated for each phone. • You can also define an authentication string for an individual SCCP IP phone by using the **capf-auth-str** command in ephone configuration mode.
Step 9	**phone-key-size** {**512** | **1024** | **2048**} **Example:** `Router(config-capf-server)# phone-key-size 2048`	(Optional) Specifies the size of the RSA key pair that is generated on the phone for the phone s certificate, in bits. • **512**—512. • **1024**—1024. This is the default. • **2048**—2048.
Step 10	**port** *tcp-port* **Example:** `Router(config-capf-server)# port 3804`	(Optional) Defines the TCP port number on which the CAPF server listens for socket connections from the phones. • *tcp-port*—TCP port number. Range is 2000 to 9999. Default is 3804.
Step 11	**keygen-retry** *number* **Example:** `Router(config-capf-server)# keygen-retry 5`	(Optional) Specifies the number of times that the server sends a key generation request. • *number*—Number of retries. Range is 0 to 100. Default is 3.
Step 12	**keygen-timeout** *minutes* **Example:** `Router(config-capf-server)# keygen-timeout 45`	(Optional) Specifies the amount of time that the server waits for a key generation response from the phone. • *minutes*—Number of minutes before the generation process times out. Range is 1 to 120. Default is 30.

	Command or Action	Purpose
Step 13	**cert-oper** {**delete all** | **fetch all** | **upgrade all**} **Example:** `Router(config-capf-server)# cert-oper upgrade all`	(Optional) Initiates the indicated certificate operation on all configured endpoints in the system. • **delete all—**Remove all phone certificates. • **fetch all—**Retrieve all phone certificates for troubleshooting. • **upgrade all—**Upgrade all phone certificates. • This command can also be configured in ephone configuration mode to initiate certificate operations on individual phones. This command in ephone configuration mode has priority over this command in CAPF-server configuration mode.
Step 14	**end** **Example:** `Router(config-capf-server)# end`	Returns to privileged EXEC mode.

Verify the CAPF Server

Use the **show capf-server summary** command to display CAPF-server configuration information.

```
Router# show capf-server summary

CAPF Server Configuration Details
        Trustpoint for TLS With Phone: tp1
        Trustpoint for CA operation: ra1
        Source Address: 10.10.10.1
        Listening Port: 3804
        Phone Key Size: 1024
        Phone KeyGen Retries: 3
        Phone KeyGen Timeout: 30 minutes
```

Configure Ephone Security Parameters

To configure security parameters for individual phones, perform the following steps for each phone.

Before You Begin

- Phones to be configured for security must be configured for basic calling in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **capf-ip-in-cnf**
5. **device-security-mode** {**authenticated** | **none** | **encrypted** }
6. **codec** {**g711ulaw** | **g722r64** | **g729r8** [**dspfarm-assist**]}
7. **capf-auth-str** *digit-string*
8. **cert-oper** {**delete** | **fetch** | **upgrade**} **auth-mode** {**auth-string** | **LSC** | **MIC** | **null-string**}
9. **reset**
10. **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** *phone-tag* **Example:** `Router(config)# ephone 24`	Enters ephone configuration mode. • *phone-tag*—Unique identifier of phone to be configured.
Step 4	**capf-ip-in-cnf** **Example:** `Router(config-ephone)# capf-ip-in-cnf`	(Optional) Enables the CAPF Server IP Address to be added to the CNF file for an SCCP phone. Upon successful registration, the SCCP phone downloads the LSC from the CAPF server. This CLI command is optional and required only if the phone has to register, download, and authenticate with the LSC.
Step 5	**device-security-mode** {**authenticated** | **none** | **encrypted** } **Example:** `Router(config-ephone)# device-security-mode authenticated`	(Optional) Enables security mode for an individual SCCP IP phone. • **authenticated—**Instructs device to establish a TLS connection with no encryption. There is no Secure Real-Time Transport Protocol (SRTP) in the media path. • **none—**SCCP signaling is not secure. This is the default. • **encrypted—**Instructs device to establish an encrypted TLS connection to secure media path using SRTP.

	Command or Action	Purpose
		• This command can also be configured in telephony-service configuration mode. The value set in ephone configuration mode has priority over the value set in telephony-service configuration mode.
Step 6	**codec** {**g711ulaw** | **g722r64** | **g729r8** [**dspfarm-assist**]} **Example:** `Router(config-ephone)# codec g711ulaw dspfarm-assist`	(Optional) Sets the security mode for SCCP signaling for a phone communicating with the Cisco Unified CME router. • **dspfarm-assist**—Required for secure transcoding with Cisco Unified CME. Causes the system to attempt to use DSP Farm resources for transcoding the segment between the phone and the Cisco Unified CME router if G.711 is negotiated for the call. This keyword is ignored if the SCCP endpoint type is ATA, VG224, or VG248.
Step 7	**capf-auth-str** *digit-string* **Example:** `Router(config-ephone)# capf-auth-str 2734`	(Optional) Defines a string to use as a personal identification number (PIN) for CAPF authentication. **Note** For instructions on how to enter the string on a phone, see Enter the Authentication String on the Phone, on page 625. • *digit-string*—Digits that the phone user must dial for CAPF authentication. The length of string is 4 to 10 digits. • This command can also be configured in telephony-service configuration mode. The value set in ephone configuration mode has priority over the value set in telephony-service configuration mode. • You can also define a PIN for CAPF authentication by using the**auth-string** command in CAPF-server configuration mode.
Step 8	**cert-oper** {**delete** | **fetch** | **upgrade**} **auth-mode** {**auth-string** | **LSC** | **MIC** | **null-string**} **Example:** `Router(config-ephone)# cert-oper upgrade auth-mode auth-string`	(Optional) Initiates the indicated certificate operation on the ephone being configured. • **delete**—Removes the phone certificate. • **fetch**—Retrieves the phone certificate for troubleshooting. • **upgrade**—Upgrades the phone certificate. • **auth-mode**—Type of authentication to use during CAPF sessions to verify endpoints that request certificates. • **auth-string**—Authentication string to be entered on the phone by the phone user. Use the **capf-auth-str** command to configure the auth-string. For configuration information, see Enter the Authentication String on the Phone, on page 625. • **LSC**—Phone provides its phone certificate for authentication. Precedence is given to an LSC if one exists. • **MIC**—Phone provides its phone certificate for authentication. Precedence is given to an MIC if one exists. MIC s issuer certificate must be imported into a PKI trustpoint. For information, see Manually Import the MIC Root Certificate, on page 626.

	Command or Action	Purpose
		• **null-string—**No authentication. • This command can also be configured in CAPF-server configuration mode to initiate certificate operations at a global level. This command in ephone configuration mode has priority over this command in CAPF-server configuration mode. • You can also use the **auth-mode** command in CAPF-server configuration mode to configure authentication at a global level.
Step 9	**reset** **Example:** `Router(config-ephone)# reset`	Performs a complete reboot of the phone.
Step 10	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verify Ephone Security Parameters

Use the **show capf-server auth-string** command to display configured authentication strings (PINs) that users enter at the phone to establish CAPF authentication.

Example:

```
Router# show capf-server auth-string

  Authentication Strings for configured Ephones
  Mac-Addr        Auth-String
  --------        -----------
  000CCE3A817C    2734
  001121116BDD    922
  000D299D50DF    9182
  000ED7B10DAC    3114
  000F90485077    3328>
  0013C352E7F1    0678
```

What to Do Next

- When you have more than one Cisco Unified CME router in your network, you must configure a CTL provider on each Cisco Unified CME router that is not running the CTL client. To configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running, see Configure the CTL Provider, on page 619.

- If the CA is a third-party CA or if the Cisco IOS CA is on a Cisco IOS router external to the Cisco Unified CME router, you must configure an RA to issue certificates to phones. For information, see Configure the Registration Authority, on page 621.
- If the specified authentication mode for the CAPF session is authentication-string, you must enter an authentication string on each phone that is receiving an updated LSC. For information, see Enter the Authentication String on the Phone, on page 625.
- If the specified authentication mode for the CAPF session is MIC, the MIC's issuer certificate must be imported into a PKI trustpoint. For information, see Manually Import the MIC Root Certificate, on page 626.
- To configure Media Encryption, see Configure Media Encryption (SRTP) in Cisco Unified CME, on page 629.

Configure the CTL Provider

When you have more than one Cisco Unified CME router in your network, you must configure a CTL provider on each Cisco Unified CME router that is not running the CTL client. To configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **credentials**
4. **ip source-address** [*ip-address* [**port** [*port-number*]]]
5. **trustpoint** *trustpoint-label*
6. **ctl-service admin username secret {0 | 1 }** *password-* string
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	**credentials** **Example:** `Router(config)# credentials`	Enters credentials-interface mode to configure a CTL provider.

	Command or Action	Purpose
Step 4	**ip source-address** [*ip-address* [**port** [*port-number*]]] **Example:** `Router(config-credentials)# ip source-address 172.19.245.1 port 2444`	identifies the local router on which this CTL provider is being configured. • *ip-address*—Typically one of the addresses of the Ethernet port of the router. • **port** *port-number*—TCP port for credentials service communication. Default is 2444 and we recommend that you use the default value.
Step 5	**trustpoint** *trustpoint-label* **Example:** `Router(config-credentials)# trustpoint ctlpv`	Configures the trustpoint. • *trustpoint-label*—Name of CTL provider trustpoint to be used for TLS sessions with the CTL client.
Step 6	**ctl-service admin username secret {0 | 1 }** *password-* string **Example:** `Router(config-credentials)# ctl-service admin user4 secret 0 c89L8o`	Specifies a username and password to authenticate the CTL client when it connects to retrieve the credentials during the CTL protocol. • *username*—Name that will be used to authenticate the client. • **secret**—Character string for login authentication and whether the string should be encrypted when it is stored in the running configuration. ◦ **0**—Not encrypted. ◦ **1**—Encrypted using Message Digest 5 (MD5). • *password-string*—Character string for login authentication.
Step 7	**end** **Example:** `Router(config-credentials)# end`	Returns to privileged EXEC mode.

Verify the CTL Provider

Use the **show credentials** command to display credentials settings.

Example:

```
Router# show credentials

Credentials IP: 172.19.245.1
```

```
Credentials PORT: 2444
Trustpoint: ctlpv
```

What to Do Next

- If the CA is a third-party CA or if the Cisco IOS CA is on a Cisco IOS router external to the Cisco Unified CME router, you must configure an RA to issue certificates to phones. For information, see Configure the Registration Authority, on page 621.
- If the specified authentication mode for the CAPF session is authentication-string, you must enter an authentication string on each phone that is receiving an updated LSC. For information, see Enter the Authentication String on the Phone, on page 625.
- If the specified authentication mode for the CAPF session is MIC, the MIC's issuer certificate must be imported into a PKI trustpoint. For information, see Manually Import the MIC Root Certificate, on page 626.
- To configure Media Encryption, see Configure Media Encryption (SRTP) in Cisco Unified CME, on page 629.

Configure the Registration Authority

A registration authority (RA) is the authority charged with recording or verifying some or all of the data required for the CA to issue certificates. In many cases the CA undertakes all of the RA functions itself, but where a CA operates over a wide geographical area or when there is security concern over exposing the CA at the edge of the network, it may be advisable to delegate some of the tasks to an RA and let the CA concentrate on its primary tasks of signing certificates.

You can configure a CA to run in RA mode. When the RA receives a manual or Simple Certificate Enrollment Protocol (SCEP) enrollment request, the administrator can either reject or grant it on the basis of local policy. If the request is granted, it is forwarded to the issuing CA, and the CA automatically generates the certificate and returns it to the RA. The client can later retrieve the granted certificate from the RA.

To configure an RA, perform the following steps on the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **revocation-check** *method1* [*method2* [*method3*]]
6. **serial-number** [**none**]
7. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
8. **exit**
9. **crypto pki server** *label*
10. **mode ra**
11. **lifetime certificate** *time*
12. **grant auto**
13. **no shutdown**
14. **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	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint ra12`	Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode. • *label*—Name for the trustpoint and RA. **Tip** This label is also required for the **cert-enroll-trustpoint** command when you set up the CA proxy. See Configure the CAPF Server, on page 612.
Step 4	**enrollment url** *ca-url* **Example:** `Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com`	Specifies the enrollment URL of the issuing CA (root CA). • *ca-url*—URL of the router on which the root CA has been installed.
Step 5	**revocation-check** *method1* [*method2* [*method3*]]	(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified,

	Command or Action	Purpose
	Example: `Router(config-ca-trustpoint)# revocation-check none`	each method is used only if the previous method returns an error, such as a server being down. Valid values for *methodn* are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an Online Certificate Status Protocol (OCSP) server.
Step 6	**serial-number** [**none**] **Example:** `Router(config-ca-trustpoint)# serial-number`	(Optional) Specifies whether the router serial number should be included in the certificate request. When this command is not used, you are prompted for the serial number during certificate enrollment. • **none**—(Optional) A serial number is not included in the certificate request.
Step 7	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(config-ca-trustpoint)# rsakeypair exampleCAkeys 1024 1024`	(Optional) Specifies an RSA key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is used. • *key-size*—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. • Multiple trustpoints can share the same key.
Step 8	**exit** **Example:** `Router(config-ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.
Step 9	**crypto pki server** *label* **Example:** `Router(config)# crypto pki server ra12`	Defines a label for the certificate server and enters certificate-server configuration mode. • *label*—Name for the trustpoint and RA. Use the same label that you previously created as a trustpoint and RA in Step 3, on page 622.
Step 10	**mode ra** **Example:** `Router(config-cs-server)# mode ra`	Places the PKI server into certificate-server mode for the RA.
Step 11	**lifetime certificate** *time*	(Optional) Specifies the lifetime, in days, of a certificate.

	Command or Action	Purpose
	Example: `Router(config-cs-server)# lifetime certificate 1800`	• *time*—Number of days until the certificate expires. Range is 1 to 1825. Default is 365. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate. • This command must be used before the server is enabled with the **no shutdown** command.
Step 12	**grant auto** **Example:** `Router(config-cs-server)# grant auto`	Allows a certificate to be issued automatically to any requester. • Configure this command only during enrollment when testing and building simple networks. • As a security best practice, use the **no grant auto** command to disable this functionality after configuration so that certificates are not continually granted.
Step 13	**no shutdown** **Example:** `Router(config-cs-server)# no shutdown`	(Optional) Enables the certificate server. • When prompted, provide input regarding acceptance of the CA certificate, the router certificate, the challenge password, and a password for protecting the private key. • Use this command only after you have completely configured your certificate server.
Step 14	**end** **Example:** `Router(config-cs-server)# end`	Returns to privileged EXEC mode.

What to Do Next

- When you have more than one Cisco Unified CME router in your network, you must configure a CTL provider on each Cisco Unified CME router that is not running the CTL client. To configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running, see Configure the CTL Provider, on page 619.
- If the specified authentication mode for the CAPF session is authentication-string, you must enter an authentication string on each phone that is receiving an updated LSC. For information, see Enter the Authentication String on the Phone, on page 625.
- If the specified authentication mode for the CAPF session is MIC, the MIC s issuer certificate must be imported into a PKI trustpoint. For information, see Manually Import the MIC Root Certificate, on page 626.
- To configure Media Encryption, see Configure Media Encryption (SRTP) in Cisco Unified CME, on page 629.

Enter the Authentication String on the Phone

This procedure is required only for the one-time installation of an LSC on a phone and only if you configured the authentication mode for the CAPF session as authentication-string. The authentication string must be communicated to the phone user so that it can be entered on the phone before the LSC is installed.

Note You can list authentication strings for phones by using the **show capf-server auth-string** command.

Restriction

- Authentication string applies for one-time use only.

Before You Begin

- Signed image exists on the IP phone; see the Cisco Unified IP phone administration documentation that supports your phone model.
- IP phone is registered in Cisco Unified CME.
- CAPF certificate exists in the CTL file. For information, see Configure the CTL Client, on page 607.
- Authentication string to be entered is configured using **auth-string** command in CAPF-server configuration mode or the **capf-auth-str** command in ephone configuration mode. For information, see Configure Telephony-Service Security Parameters, on page 604.
- The **device-security-mode** command is configured using the **none** keyword. For information, see Configure Telephony-Service Security Parameters, on page 604.

Step 1 Press the **Settings** button. On the Cisco Unified IP Phone 7921, press **Down Arrow** to access the **Settings** menu.

Step 2 If the configuration is locked, press **# (asterisk, asterisk, pound sign) to unlock it.

Step 3 Scroll down the **Settings** menu. Highlight Security Configuration and press the **Select** softkey.

Step 4 Scroll down the **Security Configuration** menu. Highlight LSC and press the **Update** softkey. On the Cisco Unified IP Phone 7921, press **# to unlock the Security Configuration menu.

Step 5 When prompted for the authentication string, enter the string provided by the system administrator and press the **Submit** softkey.
The phone installs, updates, deletes, or fetches the certificate, depending on the CAPF configuration.

You can monitor the progress of the certificate operation by viewing the messages that display on the phone. After you press **Submit**, the message “Pending” appears under the LSC option. The phone generates the public and private key pair and displays the information on the phone. When the phone successfully completes the process, the phone displays a successful message. If the phone displays a failure message, you entered the wrong authentication string or did not enable the phone for upgrade.

You can stop the process by choosing Stop at any time.

Step 6 Verify that the certificate was installed on the phone. From the **Settings** menu on the phone screen, choose **Model Information** and then press the **Select** softkey to display the Model Information.

Step 7 Press the navigation button to scroll to LSC. The value for this item indicates whether LSC is Installed or Not Installed.

What to Do Next

- When you have more than one Cisco Unified CME router in your network, you must configure a CTL provider on each Cisco Unified CME router that is not running the CTL client. To configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running, see Configure the CTL Provider, on page 619.
- If the CA is a third-party CA or if the Cisco IOS CA is on a Cisco IOS router external to the Cisco Unified CME router, you must configure an RA to issue certificates to phones. For information, see Configure the Registration Authority, on page 621 .
- If the specified authentication mode for the CAPF session is MIC, the MIC's issuer certificate must be imported into a PKI trustpoint. For information, see Manually Import the MIC Root Certificate, on page 626.
- To configure Media Encryption, see Configure Media Encryption (SRTP) in Cisco Unified CME, on page 629.

Manually Import the MIC Root Certificate

The MIC root certificate must be present in the Cisco Unified CME router to allow Cisco Unified CME to authenticate the MIC that is presented to it. To manually import the MIC root certificate on the Cisco Unified CME router, perform the following steps for each type of phone that requires a MIC for authentication.

Before You Begin

One of the following must be true before you perform this task:

- The **device-security-mode** command is configured using the **none** keyword. For information, see Configure Telephony-Service Security Parameters, on page 604.
- MIC is the specified authentication mode for phone authentication during a CAPF session.
- A phone's MIC, rather than an LSC, is used to establish the TLS session for SCCP signaling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **revocation-check none**
5. **enrollment terminal**
6. **exit**
7. **crypto pki authenticate** *name*
8. Download the four MIC root certificate files. Cut and paste the appropriate text for each certificate. Accept the certificates.
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint sanjose1`	Declares the CA that your router should use and enters ca-trustpoint configuration mode. • *name*—Already-configured label for the CA.
Step 4	**revocation-check none** **Example:** `Router(ca-trustpoint)# revocation-check none`	Specifies that revocation check is not performed and the certificate is always accepted.
Step 5	**enrollment terminal** **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual (copy-and-paste) certificate enrollment.
Step 6	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.

	Command or Action	Purpose
Step 7	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate sanjose1`	Authenticates the CA by getting the certificate from the CA. • *name*- Already-configured label for the CA.
Step 8	Download the four MIC root certificate files. Cut and paste the appropriate text for each certificate. Accept the certificates.	**1** Click on the link to the certificate: The certificates are available at the following links: • CAP-RTP-001: http://www.cisco.com/security/pki/certs/CAP-RTP-001.cer • CAP-RTP-002: http://www.cisco.com/security/pki/certs/CAP-RTP-002.cer • CMCA: http://www.cisco.com/security/pki/certs/cmca.cer • CiscoRootCA2048: http://www.cisco.com/security/pki/certs/crca2048.cer **2** When the **Downloading Certificate** dialog window opens, select the option to view the certificate. Do not install the certificate. **3** Select the **Detail** tab on top. **4** Click **Export** on the bottom and save the certificate into a file. **5** Open the file with WordPad. **6** Cut and paste the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- into the IOS console. **7** When prompted, press **Enter** and type quit. After pasting the certificate, press **Enter** and type quit on a line by itself. **8** Enter y to accept the certificate. The system responds to the pasted certificate text by providing the MD5 and SHA1 fingerprints, and asks whether you accept the certificate. Enter y to accept the certificate or n to reject it. **9** Repeat steps a. through h. for each certificate.
Step 9	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

What to Do Next

- When you have more than one Cisco Unified CME router in your network, you must configure a CTL provider on each Cisco Unified CME router that is not running the CTL client. To configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running, see Configure the CTL Provider, on page 619.
- If the CA is a third-party CA or if the Cisco IOS CA is on a Cisco IOS router external to the Cisco Unified CME router, you must configure an RA to issue certificates to phones. For information, see Configure the Registration Authority, on page 621.
- If the specified authentication mode for the CAPF session is authentication-string, you must enter an authentication string on each phone that is receiving an updated LSC. For information, see Enter the Authentication String on the Phone, on page 625.
- To configure Media Encryption, see Configure Media Encryption (SRTP) in Cisco Unified CME, on page 629.

Configure Media Encryption (SRTP) in Cisco Unified CME

To configure the network for secure calls between Cisco Unified CME systems across an H.323 trunk, perform the following steps on the Cisco Unified CME router.

Restriction

- Secure three-way software conferencing is not supported. A secure call beginning with SRTP always falls back to nonsecure Real-Time Transport Protocol (RTP) when it is joined to a conference.
- If a party drops from a three-party conference, the call between the remaining two parties returns to secure if the two parties are SRTP-capable local Skinny Client Control Protocol (SCCP) endpoints to a single Cisco Unified CME and the conference creator is one of the remaining parties. If either of the two remaining parties are only RTP-capable, the call remains nonsecure. If the two remaining parties are connected through FXS, PSTN, or VoIP, the call remains nonsecure.
- Calls to Cisco Unity Express are not secure.
- Music on Hold (MOH) is not secure.
- Video calls are not secure.
- Modem relay and T.3 fax relay calls are not secure.
- Media flow-around is not supported for call transfer and call forward.
- Conversion between inband tone and RFC 2833 DTMF is not supported. RFC 2833 DTMF handling is supported when encryption keys are sent to secure DSP Farm devices but is not supported for codec passthrough.
- Secure Cisco Unified CME does not support SIP trunks; only H.323 trunks are supported.
- Media Encryption (SRTP) supports secure supplementary services in both H.450 and non-H.450 Cisco Unified CME networks. A secure Cisco Unified CME network should be either H.450 or non-H.450, not a hybrid.
- Secure calls are supported in the default session application only.

Before You Begin

- Cisco Unified CME 4.2 or a later version.
- To make secure H.323 calls, telephony-service security parameters must be configured. See Configure Telephony-Service Security Parameters, on page 604.
- Compatible Cisco IOS Release on the Cisco VG224 Analog Phone Gateway. For information, see Cisco Unified CME and Cisco IOS Release Compatibility Matrix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **supplementary-service media-renegotiate**
5. **srtp fallback**
6. **h323**
7. **emptycapability**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode. • The **voip** keyword specifies VoIP encapsulation.
Step 4	**supplementary-service media-renegotiate** **Example:** `Router(conf-voi-serv)# supplementary-service media-renegotiate`	Enables midcall renegotiation of SRTP cryptographic keys.
Step 5	**srtp fallback** **Example:** `Router(conf-voi-serv)# srtp fallback`	Globally enables secure calls using SRTP for media encryption and authentication and enables SRTP-to-RTP fallback to support supplementary services such as ringback tone and MOH.

	Command or Action	Purpose
		• Skip this step if you are going to configure fallback on individual dial peers. • This command can also be configured in dial-peer configuration mode. This command in dial-peer configuration command takes precedence over this command in voice service voip configuration mode.
Step 6	**h323** **Example:** `Router(conf-voi-serv)# h323`	Enters H.323 voice-service configuration mode.
Step 7	**emptycapability** **Example:** `Router(conf-serv-h323)# emptycapability`	Eliminates the need for identical codec capabilities for all dial peers in the rotary group.
Step 8	**exit** **Example:** `Router(conf-serv-h323)# exit`	Exits H.323 voice-service configuration mode.

What to Do Next

You have completed the required task for configuring Media Encryption (SRTP) on Cisco Unified CME. Configuring Cisco Unified CME SRTP Fallback for H.323 Dial Peers. You can now perform the following optional tasks:

- Configure Cisco Unified CME SRTP Fallback for H.323 Dial Peers, on page 631(Optional)
- Configure Cisco Unity for Secure Cisco Unified CME Operation, on page 633(Optional)

Configure Cisco Unified CME SRTP Fallback for H.323 Dial Peers

To configure SRTP fallback for an individual dial peer, perform the following steps on the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class codec** *tag*
4. **codec preference** *value codec-type*
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **srtp fallback**
8. **voice-class codec** *tag*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice class codec** *tag* **Example:** `Router(config)# voice class codec 1`	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.
Step 4	**codec preference** *value codec-type* **Example:** `Router(config-voice-class)# codec preference 1 g711alaw`	Specifies a list of preferred codecs to use on a dial peer. • Repeat this step to build a list of preferred codecs. • Use the same preference order for the codec list on both Cisco Unified CMEs on either side of the H.323 trunk.
Step 5	**exit** **Example:** `Router(config-voice-class)# exit`	Exits voice-class configuration mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 101 voip`	Enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 7	**srtp fallback** **Example:** `Router(config-dial-peer)# srtp fallback`	Enables secure calls that use SRTP for media encryption and authentication and specifies fallback capability. • Using the **no srtp** command disables SRTP and causes the dial peer to fall back to RTP mode. • **fallback—**Enables fallback to nonsecure mode (RTP) on an individual dial peer. The **no srtp fallback** command disables fallback and SRTP. • This command can also be configured in voice service voip configuration mode. This command in dial-peer configuration command takes precedence over this command in voice service voip configuration mode.
Step 8	**voice-class codec** *tag* **Example:** `Router(config-dial-peer)# voice-class codec 1`	Assigns a previously configured codec selection preference list (codec voice class) to a Voice over IP (VoIP) dial peer. • The *tag* argument in this step is the same as the *tag* in Step 3.
Step 9	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer voice configuration mode.

Configure Cisco Unity for Secure Cisco Unified CME Operation

This section contains the following tasks:

Prerequisites for Configuring Cisco Unity for Secure Cisco Unified CME Operation

- Cisco Unity 4.2 or later version.

Configure Integration Between Cisco Unified CME and Cisco Unity

To change the settings for the integration between Cisco Unified CME and Cisco Unity, perform the following steps on the Cisco Unity server:

Step 1 If Cisco Unity Telephony Integration Manager (UTIM) is not yet open on the Cisco Unity server, choose**Programs** > **Cisco Unity** > **Manage Integrations** from the Windows Start menu. The UTIM window appears.

Step 2 In the left pane, double-click **Cisco Unity Server**. The existing integrations appear.

Step 3 Click **Cisco Unified Communications Manager** integration.

Step 4 In the right pane, click the cluster for the integration.

Step 5 Click the **Servers** tab.

Step 6 In the Cisco Unified Communications Manager Cluster Security Mode field, click the applicable setting.

Step 7 If you clicked **Non-secure**, click **Save** and skip the remaining steps in this procedure.
If you clicked **Authenticated** or **Encrypted**, the Security tab and the Add TFTP Server dialog box appear. In the IP Address or Host Name field of the Add TFTP Server dialog box, enter the IP address (or DNS name) of the primary TFTP server for the Cisco Unified Communications Manager cluster and click **OK**.

Step 8 If there are more TFTP servers that Cisco Unity will use to download the Cisco Unified Communications Manager certificates, click **Add**. The Add TFTP Server dialog box appears.

Step 9 In the IP Address or Host Name field, enter the IP address (or DNS name) of the secondary TFTP server for the Cisco Unified Communications Manager cluster and click **OK**.

Step 10 Click **Save**.
Cisco Unity creates the voice messaging port device certificates, exports the Cisco Unity server root certificate, and displays the Export Cisco Unity Root Certificate dialog box.

Step 11 Note the filename of the exported Cisco Unity server root certificate and click **OK**.

Step 12 On the Cisco Unity server, navigate to the CommServer\SkinnyCerts directory.

Step 13 Locate the Cisco Unity server root certificate file that you exported in Step 11.

Step 14 Right-click the file and click **Rename**.

Step 15 Change the file extension from .0 to .pem. For example, change the filename “12345.0” to “12345.pem” for the exported Cisco Unity server root certificate file.

Step 16 Copy this file to a PC from which you can access the Cisco Unified CME router.

Import the Cisco Unity Root Certificate to Cisco Unified CME

To import the Cisco Unity root certificate to Cisco Unified CME, perform the following steps on the Cisco Unified CME router:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **revocation-check none**
5. **enrollment terminal**
6. **exit**
7. **crypto pki authenticate** *trustpoint-label*
8. Open the root certificate file that you copied from the Cisco Unity Server in Step 16, on page 634.
9. You will be prompted to enter the CA certificate. Cut and paste the entire contents of the base 64 encoded certificate between BEGIN CERTIFICATE and END CERTIFICATE at the command line. Press **Enter** and type quit. The router prompts you to accept the certificate. Enter yes to accept the certificate.

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	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint PEM`	Declares the trustpoint that your RA mode certificate server should use and enters ca-trustpoint configuration mode. • *label*—Name for the trustpoint and RA.
Step 4	**revocation-check none** **Example:** `Router(ca-trustpoint)# revocation-check none`	(Optional) Specifies that certificate checking is not required.
Step 5	**enrollment terminal** **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment.
Step 6	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.

	Command or Action	Purpose
Step 7	**crypto pki authenticate** *trustpoint-label* **Example:** `Router(config)# crypto pki authenticate pem`	Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint when prompted. • *trustpoint-label*—Already-configured name for the trustpoint and RA. See Step 3, on page 635.
Step 8	Open the root certificate file that you copied from the Cisco Unity Server in Step 16, on page 634.	
Step 9	You will be prompted to enter the CA certificate. Cut and paste the entire contents of the base 64 encoded certificate between BEGIN CERTIFICATE and END CERTIFICATE at the command line. Press **Enter** and type quit. The router prompts you to accept the certificate. Enter yes to accept the certificate.	Completes the copying of the Cisco Unity root certificate to the Cisco Unified CME router.

Configure Cisco Unity Ports for Secure Registration

To configure Cisco Unity ports for registration in secure mode, perform the following steps:

Step 1 Choose the Cisco voice-mail port that you want to update.

Step 2 From the Device Security Mode drop-down list, choose **Encrypted**.

Step 3 Click **Update**.

Verify that Cisco Unity are Registering Securely

Use the **show sccp connections** command to verify that Cisco Unity ports are registered securely with Cisco Unified CME.

In the following example, the secure value of the type field shows that the connections are secure.

```
Router# show sccp connections

  sess_id    conn_id    stype        mode     codec   ripaddr rport sport

  16777222   16777409   secure-xcode sendrecv g729b 10.3.56.120   16772 19534
  16777222   16777393   secure-xcode sendrecv g711u 10.3.56.50    17030 18464

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

HTTPS Provisioning for Cisco Unified IP Phones

To provision a Cisco Unified IP phone for secure access to web content using HTTPS, perform the following steps:

Before You Begin

- Firmware 9.0 (4) or a later version must be installed on the IP phone to prevent an infinite registration loop.
- Certificate file to be imported from flash memory to the IP phone must be in privacy-enhanced mail format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **database level** {**minimum** | **names** |**complete**}
6. **database url** *root url*
7. **grant auto**
8. **exit**
9. **crypto pki trustpoint** *name*
10. **enrollment url** *url*
11. **exit**
12. **crypto pki server** *cs-label*
13. **no shutdown**
14. **exit**
15. **crypto pki trustpoint** *name*
16. **enrollment url** *url*
17. **revocation-check** *method1* [*method2*[*method3*]]
18. **rsakeypair** *key-label*
19. **exit**
20. **crypto pki authenticate** *name*
21. **crypto pki enroll** *name*
22. **crypto pki trustpoint** *name*
23. **enrollment url** *url*
24. **revocation-check** *method1* [*method2*[*method3*]]
25. **rsakeypair** *key-label*
26. **exit**
27. **crypto pki authenticate** *name*
28. **crypto pki enroll** *name*
29. **ctl-client**
30. **sastl trustpoint** *label*
31. **sast2 trustpoint** *label*
32. **import certificate** *tag description* **flash:** *cert_name*
33. **server application server address trustpoint label**
34. **regenerate**
35. **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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the HTTP server on the Cisco Unified CME router.
Step 4	**crypto pki server** *cs-label* **Example:** `Router(config)# crypto pki server IOS-CA`	Enables a Cisco IOS certificate server and enters certificate server configuration mode. • *cs-label*—Name of the certificate server. **Note** The certificate server name should not exceed 13 characters.
Step 5	**database level** {**minimum** | **names** |**complete**} **Example:** `Router(cs-server)# database level complete`	Controls what type of data is stored in the certificate enrollment database. • **complete**—Each issued certificate is written to the database. If this keyword is used, you should enable the **database url** command.
Step 6	**database url** *root url* **Example:** `Router(cs-server)# database url flash:`	Specifies the location where database entries for the certificate server will be stored or published. • *root url*—Location where database entries will be written.
Step 7	**grant auto** **Example:** `Router(cs-server)# grant auto`	(Optional) Allows an automatic certificate to be issued to any requester. The recommended method and default if this command is not used is manual enrollment.
Step 8	**exit** **Example:** `Router(cs-server)# exit`	Exits certificate server configuration mode.
Step 9	**crypto pki trustpoint** *name*	Declares a trustpoint and enters ca-trustpoint configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# crypto pki trustpoint IOS-CA`	• *name*—Name for the trustpoint.
Step 10	**enrollment url** *url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.1.1.1:80`	Specifies the enrollment parameters of a certification authority. • *url*—Specifies the URL of the file system where your router should send certificate requests.
Step 11	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.
Step 12	**crypto pki server** *cs-label* **Example:** `Router(config)# crypto pki server IOS-CA`	Enables a Cisco IOS certificate server and enters certificate server configuration mode. • *cs-label*—Name of the certificate server. **Note** The certificate server name should not exceed 13 characters.
Step 13	**no shutdown** **Example:** `Router(cs-server)# no shutdown`	Enables the Cisco IOS Certification Authority.
Step 14	**exit** **Example:** `Router(cs-server)# exit`	Exits certificate server configuration mode.
Step 15	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint primary-cme`	Declares a trustpoint and enters ca-trustpoint configuration mode. • *name*—Name for the trustpoint.
Step 16	**enrollment url** *url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.1.1.1:80`	Specifies the enrollment parameters of the certification authority. • *url*—Specifies the URL of the file system where your router should send certificate requests.
Step 17	**revocation-check** *method1* [*method2*[*method3*]] **Example:** `Router(ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate. • **none**—Certificate checking is not required.
Step 18	**rsakeypair** *key-label*	Specifies which RSA key pair to associate with the certificate.

	Command or Action	Purpose
	Example: `Router(ca-trustpoint)# rsakeypair primary-cme`	• *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
Step 19	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.
Step 20	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate primary-cme`	Authenticates the certification authority by getting the authority's certificate. • *name*—Name of the certification authority.
Step 21	**crypto pki enroll** *name* **Example:** `Router(config)# crypto pki enroll primary-cme`	Obtains the certificates for the router from the certificate authority. • *name*—Name of the certification authority. Use the same name as when you declared the certification authority using the **crypto pki trustpoint** command.
Step 22	**crypto pki trustpoint** *name* **Example:** `Router(config)# crypto pki trustpoint sast-secondary`	Declares a trustpoint and enters ca-trustpoint configuration mode. • *name*—Name for the trustpoint.
Step 23	**enrollment url** *url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.1.1.1:80`	Specifies the enrollment parameters of a certification authority. • *url*—Specifies the URL of the file system where your router should send certificate requests.
Step 24	**revocation-check** *method1* [*method2*[*method3*]] **Example:** `Router(ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate. • **none**—Certificate checking is not required.
Step 25	**rsakeypair** *key-label* **Example:** `Router(ca-trustpoint)# rsakeypair sast-secondary`	Specifies which RSA key pair to associate with the certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
Step 26	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode.

	Command or Action	Purpose
Step 27	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate sast-secondary`	Authenticates the certification authority by getting the authority's certificate. • *name*—Name of the certification authority.
Step 28	**crypto pki enroll** *name* **Example:** `Router(config)# crypto pki enroll sast-secondary`	Obtains the certificates for the router from the certificate authority. • *name*—Name of the certification authority. Use the same name as when you declared the certification authority using the **crypto pki trustpoint** command.
Step 29	**ctl-client** **Example:** `Router(config)# ctl-client`	Enters CTL-client configuration mode to set parameters for the CTL client.
Step 30	**sastl trustpoint** *label* **Example:** `Router(config-ctl-client)# sast1 trustpoint first-sast`	Configures the credentials for the primary SAST. • *label*—Name of SAST1 trustpoint. **Note** SAST1 and SAST2 certificates must be different from each other. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to the factory default.
Step 31	**sast2 trustpoint** *label* **Example:** `Router(config-ctl-client)# sast2 trustpoint second-sast`	Configures the credentials for the secondary SAST. • *label*—Name of SAST2 trustpoint. **Note** SAST1 and SAST2 certificates must be different from each other. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to the factory default.
Step 32	**import certificate** *tag description* **flash:** *cert_name* **Example:** `Router(config-ctl-client)# import certificate 5 FlashCert flash:flash_cert.cer`	Imports a trusted certificate in PEM format from flash memory to the CTL file of an IP phone. **Note** This step is required to provision HTTPS service running on external server. • *tag*—identifier for the trusted certificate. • *description*—Descriptive name of the trusted certificate. • **flash:***cert_cert*—Specifies the filename of the trusted certificate stored in flash memory.
Step 33	**server application server address trustpoint label**	Configures the server application and the credentials for the SAST.

	Command or Action	Purpose
	Example: `Router(config-ctl-client)# server application 10.1.2.3 trustpoint first-sast`	
Step 34	**regenerate** **Example:** `Router(config-ctl-client)# regenerate`	Creates a new CTLFile.tlv after you make changes to the CTL client configuration.
Step 35	**end** **Example:** `Router(config-ctl-client)# end`	Exits to privileged EXEC mode.

Configuration Examples for Security

Example for Configuring Cisco IOS CA

```
crypto pki server iosca
   grant auto
   database url flash:
  !
  crypto pki trustpoint iosca
   revocation-check none
   rsakeypair iosca
  !
  crypto pki certificate chain iosca
   certificate ca 01
    308201F9 30820162 ...
```

Example for Manually Importing MIC Root Certificate on the Cisco Unified CME Router

The following example shows three certificates imported to the router (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 have been granted. The five certificates include the three certificates just entered, the CA server certificate, and the 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
```

Example for Configuring Telephony-Service Security Parameters

The following example shows Cisco Unified CME security parameters:

```
telephony-service
 device-security-mode authenticated
 secure-signaling trustpoint cme-sccp
 tftp-server-credentials trustpoint cme-tftp
 load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign create

ephone 24
 device-security-mode authenticated
 capf-auth-str 2734
 cert-oper upgrade auth-mode auth-string
```

Example for Configuring CTL Client Running on Cisco Unified CME Router

```
ctl-client
 server capf 10.1.1.1 trustpoint cmeserver
 server cme 10.1.1.1 trustpoint cmeserver
 server tftp 10.1.1.1 trustpoint cmeserver
 sast1 trustpoint cmeserver
 sast2 trustpoint sast2 CTL Client Running on Another Router: Example
ctl-client
 server cme 10.1.1.100 trustpoint cmeserver
 server cme 10.1.1.1 username cisco password 1 0822455D0A16544541
 sast1 trustpoint cmeserver
 sast2 trustpoint sast1 CAPF Server: Example
!
ip dhcp pool cme-pool
   network 10.1.1.0 255.255.255.0
   option 150 ip 10.1.1.1
   default-router 10.1.1.1
!
capf-server
 port 3804
 auth-mode null-string
 cert-enroll-trustpoint iosra password 1 00071A1507545A545C
 trustpoint-label cmeserver
 source-addr 10.1.1.1
!
crypto pki server iosra
 grant auto
 mode ra
 database url slot0:
!
crypto pki trustpoint cmeserver
 enrollment url http://10.1.1.100:80
 serial-number
 revocation-check none
 rsakeypair cmeserver
!
```

```
crypto pki trustpoint sast2
 enrollment url http://10.1.1.100:80
 serial-number
 revocation-check none
 rsakeypair sast2
!
!
crypto pki trustpoint iosra
   enrollment url http://10.1.1.200:80
   revocation-check none
   rsakeypair iosra
  !
  !
  crypto pki certificate chain cmeserver
   certificate 1B
    30820207 30820170 A0030201 0202011B 300D0609 2A864886 F70D0101 04050030
    ....
    quit
   certificate ca 01
    3082026B 308201D4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    ...
    quit
  crypto pki certificate chain sast2
   certificate 1C
    30820207 30820170 A0030201 0202011C 300D0609 2A864886 F70D0101 04050030
    ....
    quit
   certificate ca 01
    3082026B 308201D4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    .....
    quit
  crypto pki certificate chain capf-tp
  crypto pki certificate chain iosra
   certificate 04
    30820201 3082016A A0030201 02020104 300D0609 2A864886 F70D0101 04050030
    ......
   certificate ca 01
    308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    ....
    quit
  !
  !
  credentials
   ctl-service admin cisco secret 1 094F471A1A0A464058
   ip source-address 10.1.1.1 port 2444
   trustpoint cmeserver
  !
  !
  telephony-service
   no auto-reg-ephone
   load 7960-7940 P00307010200
   load 7914 S00104000100
   load 7941GE TERM41.7-0-0-129DEV
   load 7970 TERM70.7-0-0-77DEV
   max-ephones 20
   max-dn 10
   ip source-address 10.1.1.1 port 2000 secondary 10.1.1.100
   secure-signaling trustpoint cmeserver
   cnf-file location flash:
   cnf-file perphone
   dialplan-pattern 1 2... extension-length 4
   max-conferences 8 gain -6
   transfer-pattern ....
   tftp-server-credentials trustpoint cmeserver
   server-security-mode secure
   device-security-mode encrypted
   load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign
   load-cfg-file slot0:P00307010200.bin alias P00307010200.bin
   load-cfg-file slot0:P00307010200.loads alias P00307010200.loads
   load-cfg-file slot0:P00307010200.sb2 alias P00307010200.sb2
   load-cfg-file slot0:P00307010200.sbn alias P00307010200.sbn
   load-cfg-file slot0:cnu41.2-7-4-116dev.sbn alias cnu41.2-7-4-116dev.sbn
```

```
 load-cfg-file slot0:Jar41.2-9-0-101dev.sbn alias Jar41.2-9-0-101dev.sbn
 load-cfg-file slot0:CVM41.2-0-0-96dev.sbn alias CVM41.2-0-0-96dev.sbn
 load-cfg-file slot0:TERM41.DEFAULT.loads alias TERM41.DEFAULT.loads
 load-cfg-file slot0:TERM70.DEFAULT.loads alias TERM70.DEFAULT.loads
 load-cfg-file slot0:Jar70.2-9-0-54dev.sbn alias Jar70.2-9-0-54dev.sbn
 load-cfg-file slot0:cnu70.2-7-4-58dev.sbn alias cnu70.2-7-4-58dev.sbn
 load-cfg-file slot0:CVM70.2-0-0-49dev.sbn alias CVM70.2-0-0-49dev.sbn
 load-cfg-file slot0:DistinctiveRingList.xml alias DistinctiveRingList.xml sign
 load-cfg-file slot0:Piano1.raw alias Piano1.raw sign
 load-cfg-file slot0:S00104000100.sbn alias S00104000100.sbn
 create cnf-files version-stamp 7960 Aug 13 2005 12:39:24
!
!
ephone  1
 device-security-mode encrypted
 cert-oper upgrade auth-mode null-string
 mac-address 000C.CE3A.817C
 type 7960 addon 1 7914
 button  1:2 8:8
!
!
ephone  2
 device-security-mode encrypted
 capf-auth-str 2476
 cert-oper upgrade auth-mode null-string
 mac-address 0011.2111.6BDD
 type 7970
 button  1:1
!
!
ephone  3
 device-security-mode encrypted
 capf-auth-str 5425
 cert-oper upgrade auth-mode null-string
 mac-address 000D.299D.50DF
 type 7970
 button  1:3
!
!
ephone  4
 device-security-mode encrypted
 capf-auth-str 7176
 cert-oper upgrade auth-mode null-string
 mac-address 000E.D7B1.0DAC
 type 7960
 button  1:4
!
!
ephone  5
 device-security-mode encrypted
 mac-address 000F.9048.5077
 type 7960
 button  1:5
!
!
ephone  6
 device-security-mode encrypted
 mac-address 0013.C352.E7F1
 type 7941GE
 button  1:6
!
```

Example for Secure Unified CME

Router# **show running-config**

```
Building configuration...

Current configuration : 12735 bytes
!
```

```
! No configuration change since last restart
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
card type e1 1 1
logging queue-limit 1000
logging buffered 9999999 debugging
logging rate-limit 10000
no logging console
!
aaa new-model
!
!
aaa accounting connection h323 start-stop group radius
!
aaa session-id common
!
resource policy
!
clock timezone IST 5
no network-clock-participate slot 1
!
!
ip cef
!
!
isdn switch-type primary-net5
!
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
!
!
ctl-client
 server capf 10.13.32.11 trustpoint mytrustpoint1
 server tftp 10.13.32.11 trustpoint mytrustpoint1
 server cme 10.13.32.11 trustpoint mytrustpoint1
 sast1 trustpoint mytrustpoint1>
 sast2 trustpoint sast2
!
capf-server
 port 3804
 auth-mode null-string
 cert-enroll-trustpoint iosra password 1 mypassword
 trustpoint-label mytrustpoint1
 source-addr 10.13.32.11
 phone-key-size 512
!
voice call debug full-guid
!
voice service voip
 srtp fallback
 allow-connections h323 to h323
 no supplementary-service h450.2
 no supplementary-service h450.3
 no supplementary-service h450.7
 supplementary-service media-renegotiate
 h323
  emptycapability
  ras rrq ttl 4000
!
!
```

```
voice class codec 2
 codec preference 1 g711alaw
 codec preference 2 g711ulaw
!
voice class codec 3
 codec preference 1 g729r8
 codec preference 8 g711alaw
 codec preference 9 g711ulaw
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g728
 codec preference 3 g723ar63
 codec preference 4 g711ulaw
!
!
voice iec syslog
voice statistics type iec
voice statistics time-range since-reset
!
!
!
crypto pki server myra
 database level complete
 grant auto
 lifetime certificate 1800
!
crypto pki trustpoint myra
 enrollment url http://10.13.32.11:80
 revocation-check none
 rsakeypair iosra
!
crypto pki trustpoint mytrustpoint1
 enrollment url http://10.13.32.11:80
 revocation-check none
 rsakeypair mytrustpoint1
!
crypto pki trustpoint sast2
 enrollment url http://10.13.32.11:80
 revocation-check none
 rsakeypair sast2
!
!
crypto pki certificate chain myra
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343031
  375A170D 30393037 30363035 34303137 5A301031 0E300C06 03550403 1305696F
  73726130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  D8CE29F9 C9FDB1DD 0E1517E3 6CB4AAF7 52B83DE2 1C017ACA DFC4AF42 F9D10D08
  E74BF95B 29378902 B49E32C4 85907384 84CAE4B2 7759BB84 8AB1F578 580793C4
 B11A2DBE B2ED02CC DA0C3824 A5FCC377 18CE87EA C0C297BA BE54530F E62247D8
  1483CD14 9FD89EFE 05DFBB37 E03FD3F8 B2B1C0B8 A1931BCC B1174A9E 6566F8F5
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014B7 16F6FD67 29666C90
  D0C62515 E14265A9 EB256230 1D060355 1D0E0416 0414B716 F6FD6729 666C90D0
  C62515E1 4265A9EB 2562300D 06092A86 4886F70D 01010405 00038181 002B7F41
  64535A66 D20D888E 661B9584 5E3A28DF 4E5A95B9 97E57CAE B07A7C38 7F3B60EE
  75C7E5DE 6DF19B06 5F755FB5 190BABFC EF272CEF 865FE01B 1CE80F98 F320A569
  CAFFA5D9 3DB3E7D8 8A86C66C F227FF81 6C4449F2 AF8015D9 8129C909 81AFDC01
  180B61E8 85E19873 96DB3AE3 E6B70726 9BF93521 CA2FA906 99194ECA 8F
  quit
crypto pki certificate chain mytrustpoint1
 certificate 02
  308201AB 30820114 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343233
 385A170D 30393037 30363035 34303137 5A301A31 18301606 092A8648 86F70D01
  09021609 32383531 2D434D45 32305C30 0D06092A 864886F7 0D010101 0500034B
  00304802 4100B3ED A902646C 3851B7F6 CF94887F 0EC437E3 3B6FEDB2 2B4B45A6
  3611C243 5A0759EA 1E8D96D1 60ABE028 ED6A3F2A E95DCE45 BE0921AF 82E53E57
  17CC12F0 C1270203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 14B716F6 FD672966 6C90D0C6 2515E142 65A9EB25 62301D06
  03551D0E 04160414 4EE1943C EA817A9E 7010D5B8 0467E9B0 6BA76746 300D0609
```

```
  2A864886 F70D0101 04050003 81810003 564A6DA1 868B2669 7C096F9A 41173CFC
  E49246EE C645E30B A0753E3B E1A265D1 6EA5A829 F10CD0E8 3F2E3AD4 39D8DFE8
  83525F2B D19F5E15 F27D6262 62852D1F 43629B68 86D91B5F 7B2E2C25 3BD2CCC3
  00EF4028 714339B2 6A7E0B2F 131D2D9E 0BE08853 5CCAE47C 4F74953C 19305A20
  B2C97808 D6E01351 48366421 A1D407
  quit
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343031
  375A170D 30393037 30363035 34303137 5A301031 0E300C06 03550403 1305696F
  73726130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  D8CE29F9 C9FDB1DD 0E1517E3 6CB4AAF7 52B83DE2 1C017ACA DFC4AF42 F9D10D08
  E74BF95B 29378902 B49E32C4 85907384 84CAE4B2 7759BB84 8AB1F578 580793C4
  B11A2DBE B2ED02CC DA0C3824 A5FCC377 18CE87EA C0C297BA BE54530F E62247D8
  1483CD14 9FD89EFE 05DFBB37 E03FD3F8 B2B1C0B8 A1931BCC B1174A9E 6566F8F5
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014B7 16F6FD67 29666C90
  D0C62515 E14265A9 EB256230 1D060355 1D0E0416 0414B716 F6FD6729 666C90D0
  C62515E1 4265A9EB 2562300D 06092A86 4886F70D 01010405 00038181 002B7F41
  64535A66 D20D888E 661B9584 5E3A28DF 4E5A95B9 97E57CAE B07A7C38 7F3B60EE
  75C7E5DE 6DF19B06 5F755FB5 190BABFC EF272CEF 865FE01B 1CE80F98 F320A569
  CAFFA5D9 3DB3E7D8 8A86C66C F227FF81 6C4449F2 AF8015D9 8129C909 81AFDC01
  180B61E8 85E19873 96DB3AE3 E6B70726 9BF93521 CA2FA906 99194ECA 8F
  quit
crypto pki certificate chain sast2
 certificate 03
  308201AB 30820114 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343331
  375A170D 30393037 30363035 34303137 5A301A31 18301606 092A8648 86F70D01
  09021609 32383531 2D434D45 32305C30 0D06092A 864886F7 0D010101 0500034B
  00304802 4100C703 840B11A7 81FCE5AE A14FE593 5114D3C2 5473F488 B8FB4CC5
  41EAFA3A D99381D8 21AE6AA9 BA83A84E 9DF3E8C6 54978787 5EF6CC35 C334D55E
  A3051372 17D30203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 14B716F6 FD672966 6C90D0C6 2515E142 65A9EB25 62301D06
  03551D0E 04160414 EB2146B4 EE24AA61 8B5D2F8D 2AD3B786 CBADC8F2 300D0609
  2A864886 F70D0101 04050003 81810057 BA0053E9 8FD54B25 72D85A4C CAB47F26
  8316F494 E94DFFB9 8E9D065C 9748465C F54719CA C7724F50 67FBCAFF BC332109
  DC2FB93D 5AD86583 EDC3E648 39274CE8 D4A5F002 5F21ED3C 6D524AB7 7F5B1876
  51867027 9BD2FFED 06984558 C903064E 5552015F 289BA9BB 308D327A DFE0A3B9
  78CF2B02 2DD4C208 80CDC0A8 43A26A
  quit
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343031
  375A170D 30393037 30363035 34303137 5A301031 0E300C06 03550403 1305696F
  73726130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  D8CE29F9 C9FDB1DD 0E1517E3 6CB4AAF7 52B83DE2 1C017ACA DFC4AF42 F9D10D08
  E74BF95B 29378902 B49E32C4 85907384 84CAE4B2 7759BB84 8AB1F578 580793C4
  B11A2DBE B2ED02CC DA0C3824 A5FCC377 18CE87EA C0C297BA BE54530F E62247D8
  1483CD14 9FD89EFE 05DFBB37 E03FD3F8 B2B1C0B8 A1931BCC B1174A9E 6566F8F5
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014B7 16F6FD67 29666C90
  D0C62515 E14265A9 EB256230 1D060355 1D0E0416 0414B716 F6FD6729 666C90D0
  C62515E1 4265A9EB 2562300D 06092A86 4886F70D 01010405 00038181 002B7F41
  64535A66 D20D888E 661B9584 5E3A28DF 4E5A95B9 97E57CAE B07A7C38 7F3B60EE
  75C7E5DE 6DF19B06 5F755FB5 190BABFC EF272CEF 865FE01B 1CE80F98 F320A569
  CAFFA5D9 3DB3E7D8 8A86C66C F227FF81 6C4449F2 AF8015D9 8129C909 81AFDC01
  180B61E8 85E19873 96DB3AE3 E6B70726 9BF93521 CA2FA906 99194ECA 8F
  quit
!
!
username admin password 0 mypassword2
username cisco password 0 mypassword2
!
!
controller E1 1/0
 pri-group timeslots 1-31
!
controller E1 1/1
 pri-group timeslots 1-31
gw-accounting aaa
!
!
```

```
!
!
!
interface GigabitEthernet0/0
 ip address 10.13.32.11 255.255.255.0
 duplex auto
 speed auto
 fair-queue 64 256 32
 h323-gateway voip interface
 h323-gateway voip id GK1 ipaddr 10.13.32.13 1719
 h323-gateway voip id GK2 ipaddr 10.13.32.16 1719
 h323-gateway voip h323-id 2851-CiscoUnifiedCME
 h323-gateway voip tech-prefix 1#
 ip rsvp bandwidth 1000 100
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial1/1:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 10.13.32.1
!
!
ip http server
ip http authentication local
no ip http secure-server
ip http path flash:
!
!
!
!
!
!
tftp-server flash:music-on-hold.au
tftp-server flash:TERM70.DEFAULT.loads
tftp-server flash:TERM71.DEFAULT.loads
tftp-server flash:P00308000300.bin
tftp-server flash:P00308000300.loads
tftp-server flash:P00308000300.sb2
tftp-server flash:P00308000300.sbn
tftp-server flash:SCCP70.8-0-3S.loads
tftp-server flash:cvm70sccp.8-0-2-25.sbn
tftp-server flash:apps70.1-1-2-26.sbn
tftp-server flash:dsp70.1-1-2-26.sbn
tftp-server flash:cnu70.3-1-2-26.sbn
tftp-server flash:jar70sccp.8-0-2-25.sbn
radius-server host 10.13.32.241 auth-port 1645 acct-port 1646
radius-server timeout 40
radius-server deadtime 2
radius-server key cisco
radius-server vsa send accounting
!
control-plane
!
no call rsvp-sync
!
```

```
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/0:15
!
voice-port 1/1:15
!
!
!
!
!
dial-peer voice 1 voip
 destination-pattern ........
 voice-class codec 2
 session target ras
 incoming called-number 9362....
 dtmf-relay h245-alphanumeric
 req-qos controlled-load audio
!
dial-peer voice 2 pots
 destination-pattern 93621101
!
dial-peer voice 3 pots
 destination-pattern 93621102
!
dial-peer voice 10 voip
 destination-pattern 2668....
 voice-class codec 1
 session target ipv4:10.13.46.200
!
dial-peer voice 101 voip
 shutdown
 destination-pattern 5694....
 voice-class codec 1
 session target ipv4:10.13.32.10
 incoming called-number 9362....
!
dial-peer voice 102 voip
 shutdown
 destination-pattern 2558....
 voice-class codec 1
 session target ipv4:10.13.32.12
 incoming called-number 9362....
!
dial-peer voice 103 voip
 shutdown
 destination-pattern 9845....
 voice-class codec 1
 session target ipv4:10.13.32.14
 incoming called-number 9362....
!
dial-peer voice 104 voip
 shutdown
 destination-pattern 9844....
 voice-class codec 1
 session target ipv4:10.13.32.15
 incoming called-number 9362....
!
dial-peer voice 201 pots
 destination-pattern 93625...
 no digit-strip
 direct-inward-dial
 port 1/0:15
!
dial-peer voice 202 pots
 destination-pattern 93625...
 no digit-strip
 direct-inward-dial
 port 1/1:15
!
!
```

```
gateway
 timer receive-rtp 1200
!
!
!
telephony-service
 load 7960-7940 P00308000300
 max-ephones 4
 max-dn 4
 ip source-address 10.13.32.11 port 2000
 auto assign 1 to 4
 secure-signaling trustpoint mytrustpoint1
 cnf-file location flash:
 cnf-file perphone
 voicemail 25589000
 max-conferences 4 gain -6
call-forward pattern .T
 moh flash:music-on-hold.au
 web admin system name admin password mypassword2
 dn-webedit
 time-webedit
 transfer-system full-consult
 transfer-pattern ........
 tftp-server-credentials trustpoint mytrustpoint1
 server-security-mode secure
 device-security-mode encrypted
 create cnf-files version-stamp 7960 Oct 25 2006 07:19:39
!
!
ephone-dn  1
 number 93621000
 name 2851-PH1
 call-forward noan 25581101 timeout 10
!
!
ephone-dn  2
 number 93621001
 name 2851-PH2
 call-forward noan 98441000 timeout 10
!
!
ephone-dn  3
 number 93621002
 name 2851-PH3
!
!
ephone-dn  4
 number 93621003
 name 2851-PH4
!
!
ephone  1
       capf-ip-in-cnf
             no multicast-moh
 device-security-mode encrypted
 mac-address 0012.4302.A7CC
 type 7970
 button  1:1
!
!
!
ephone  2
             capf-ip-in-cnf
 no multicast-moh
 device-security-mode encrypted
 mac-address 0017.94CA.9CCD
 type 7960
 button  1:2
!
!
!
ephone  3
             capf-ip-in-cnf
```

```
 no multicast-moh
 device-security-mode encrypted
 mac-address 0017.94CA.9833
 type 7960
 button  1:3
!
!
!
ephone  4
             capf-ip-in-cnf
 no multicast-moh
 device-security-mode none
 mac-address 0017.94CA.A141
 type 7960
 button  1:4
!
!
!
line con 0
 logging synchronous level all limit 20480000
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
ntp clock-period 17179791
ntp server 10.13.32.12
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

Example for Configuring HTTPS Support for Cisco Unified CME

Configurations similar to the following example are required before HTTPS support for services like local-directory lookup, My Phone Apps, and Extension Mobility in Cisco Unified CME can be configured at four different levels:

```
Router(config)# ip http server
Router(config)# crypto pki server IOS-CA
Router(cs-server)# database level complete
Router(cs-server)# database url flash:
Router(cs-server)# grant auto
Router(cs-server)# exit
Router(config)# crypto pki trustpoint IOS-CA
Router(ca-trustpoint)# enrollment url http://10.1.1.1:80
Router(ca-trustpoint)# exit
Router(config)# crypto pki server IOS-CA
Router(cs-server)# no shutdown
Router(cs-server)# exit
Router(config)# crypto pki trustpoint primary-cme
Router(ca-trustpoint)# enrollment url http://10.1.1.1.80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair primary-cme
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate primary-cme
Router(config)# crypto pki enroll primary-cme
Router(config)# crypto pki trustpoint sast-secondary
Router(ca-trustpoint)# enrollment url http://10.1.1.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair sast-secondary
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate sast-secondary
Router(config)# crypto pki enroll sast-secondary
Router(config)# ctl-client
Router(config-ctl-client)# sast1 trustpoint first-sast
```

```
Router(config-ctl-client)# sast2 trustpoint second-sast
Router(config-ctl-client)# server application 10.1.2.3 trustpoint first-sast
Router(config-ctl-client)# regenerate
Router(config-ctl-client)# end
```

For Cisco Unified SCCP IP Phones at the global level:

```
configure terminal
telephony-service
     cnf-file perphone
     service https
```

For Cisco Unified SCCP IP Phones at the ephone-template level:

```
configure terminal
ephone-template 1
     service https
```

For Cisco Unified SIP IP Phones at the global level:

```
configure terminal
voice register global
     service https
```

For Cisco Unified SIP IP Phones at the voice register template level:

```
configure terminal
voice register template 1
    service https
```

Where to Go Next

PKI Management

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPsec), secure shell (SSH), and secure socket layer (SSL).

Cisco VG224 Analog Phone Gateway

- To configure secure endpoints on the Cisco VG224 Analog Phone Gateway, see the *Configuring Secure Signalling and Media Encryption on the Cisco VG224* section of Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.

Feature Information for Security

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

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

Table 40: Feature Information for Security

Feature Name	Cisco Unified CME Version	Feature Information
HTTPS Support in Cisco Unified CME	9.5	Introduces HTTPS support on Cisco Unified CME.
HTTPS Provisioning for Cisco Unified IP Phones	8.8	Allows you to import an IP phone's trusted certificate to an IP phone's CTL file using the **import certificate** command.
Media Encryption (SRTP) on Cisco Unified CME	4.2	Introduces media encryption on Cisco Unified CME.
Phone Authentication	4.0	Introduces phone authentication for Cisco Unified CME phones.

CHAPTER 18

Directory Services

Information About Directory Services

Local Directory

Cisco Unified CME automatically creates a local phone directory containing the telephone numbers that are assigned in the directory number configuration of the phone. You can make additional entries to the local directory in telephony services configuration mode. Additional entries can be nonlocal numbers such as telephone numbers on other Cisco Unified CME systems used by your company.

When a phone user selects the **Directories** > **Local Directory** menu, the phone displays a search page from Unified CME. After a user enters the search information, the phone sends the information to Cisco Unified CME, which searches for the requested number or name pattern in the directory number configuration and sends the response back to the phone, which displays the matched results. The phone can display up to 32 directory entries. If a search results in more than 32 entries, the phone displays an error message and the user must refine the search criteria to narrow the results.

The order of the names in the directory entries is first-name-first or last-name-first. Character strings for directory names can contain a spaces and a comma (,) and cannot contain an ampersand (&).

The local directory that is displayed on an IP phone is an XML page that is accessed through HTTP without password protection. The directory HTTP service can be disabled to suppress the availability of the local directory.

For configuration information, see Configure Local Directory Service, on page 661.

From CME 12.0 onwards, an optional username and password can be configured for authenticating the local directory services.

For more information on the CLI command **service local-directoryauthenticateusername password**, see Cisco Unified Communications Manager Express Command Reference.

External Directory

Cisco Unified IP Phones can support URLs in association with the four programmable feature buttons on IP phones, including the Directories button. Operation of these services is determined by the Cisco Unified IP phone capabilities and the content of the referenced URL. Provisioning the directory URL to select an external directory resource disables the Cisco Unified CME local directory service.

Called-Name Display

When phone agents answer calls for different departments or people, it is often helpful for them to see a display of the name, rather than the number of the called party. The Dialed Number Identification Service (or Called-Name Display) feature supports the display of the name associated with a called number for incoming calls to IP phones configured on a Unified CME. The display name is obtained from the list of Unified CME directory names using directory lookup.

You need to configure the CLI command **service dnis dir-lookup** under telephony-service configuration mode to use this directory lookup service. For more information on the CLI command **service dnis dir-lookup**, see Cisco Unified Communications Manager Express Command Reference Guide.

If the display name for a called number is not available in Unified CME directory names, the display name can be added using the CLI command **directory entry**. For more information on the CLI command **directory entry**, see Cisco Unified Communications Manager Express Command Reference Guide.

Note When a phone receives two simultaneous calls, there is a slight time difference between the calls being acknowledged by the phone. Called-name Display is only for the first call acknowledged by the phone. Even when the first call is disconnected and the second call is in ringing state, Called-name Display feature does not work for the second call.

For an example of Called-Name Display , see Example for Called-Name Display for Voice Hunt Group, on page 672

The called-name display feature for ephone-dns can display either of the following types of name:

- Name for a directory number in a local directory
- Name associated with an overlay directory number. Calls to the first directory number in a set of overlay numbers will display a caller ID. Calls to the remaining directory numbers in the overlay set will display the name associated with the directory number.

This is an example of Called-Name Display for ephone-dns. If order-entry agents are servicing three catalogs with individual 800 numbers configured in one overlay ephone-dn set, they need to know which catalog is being called to give the correct greeting, such as "Thank you for calling catalog *N*. May I take your order?"

From Unified CME Release 12.0 onwards, the Dialed Number Identification Service feature is supported for phones configured under voice hunt group. For information on configuring Called-Name Display feature, see Called-Name Display, on page 666.

Directory Search

Cisco Unified CME 4.3 increases the number of entries supported in a search results list from 32 to up to 240 when using the directory search feature. For example, if a user enters smith as the last name, all 240 matches are displayed on eight different pages, with 30 entries per page. If multiple pages are required, the phone displays two new softkeys, "Next" and "Prev" that the phone user can press to move back and forth between the previous and next pages. Text such as "Page 2 of 3" displays to indicate the current and total pages on the search results.

Configure Directory Services

Configure Local Directory Service

To define the format for local directory names or block the local directory display on all phones, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **directory** {**first-name-first** |**last-name-first**}
5. **no service local-directory**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**directory** {**first-name-first** |**last-name-first**}	Defines the format for entries in the local directory.

	Command or Action	Purpose
	Example: `Router(config-telephony)# directory last-name-first`	• Default is **first-name-first**.
Step 5	**no service local-directory** **Example:** `Router(config-telephony)# no service local-directory`	Disables local directory service on IP phones.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Define a Name for a Directory Number on SCCP Phone

To define a name to be used for caller-ID displays and as a local directory entry, perform the following steps.

Restriction

- The name to be associated with a directory number cannot contain special characters, such as an ampersand (&). The only special characters allowed in the name are the comma (,) and the percent sign (%).

Before You Begin

- Cisco CME 3.0 or a later version.
- Directory number for which you are defining a directory entry must already have a number assigned by using the **number (ephone- dn)** command. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **name** *name*
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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 55`	Enters ephone-dn configuration mode.

Step 4	**name** *name*
	
	Example:
	`Router(config-ephone-dn)# name Smith, John`
	or
	`Router(config-ephone-dn)# name Shipping and Handling`
		Associates a name with this directory number.
		• Must follow the name order that is specified with the directory command: first-name-first or last-name-first.
		• *name*—Alphanumeric string to be displayed.
		◦ You must separate the two parts, first last or last first, of the *name* string with a space.
		◦ The second part of the *name* string can contain spaces, such as "and Shipping". The first part of the *name* string cannot contain spaces.
		◦ You can include a comma (,) in the *name* string for display purposes, for example, when you use the last-name-first pattern (last, first).

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

Add an Entry to a Local Directory on SCCP Phone

To add an entry to the local directory, perform the following steps.

Restriction

- If the directory entry being configured is to be used for called-name display, the number being configured must contain at least one wildcard character.
- Entry for local directory cannot include opening or closing quotation marks (‘, ‘, “, or ”).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **directory entry** {*directory-tag number* **name** *name* | **clear**}
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**directory entry** {*directory-tag number* **name** *name* | **clear**} **Example:** `Router(config-telephony)#` **directory entry 1 5550111 name Sales**	Creates a telephone directory entry that is displayed on an IP phone. Entries appear in the order in which they are entered. • directory-tag—Unique sequence number that identifies this directory entry during all configuration tasks. Range is 1 to 250. • If this name is to be used for called-name display, the *number* associated with the names must contain at least one wildcard character. • *name*—1 to 24 alphanumeric characters, including spaces. Name cannot include opening or closing quotation marks (, , , or).
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure External Directory Service on SCCP Phone

To enable an external directory resource on supported Cisco Unified IP phones and disable local directory services on those same phones, perform the following steps.

Restriction

- Provisioning of the directory URL to select an external directory resource disables the Cisco Unified CME local directory service.
- Configuring external directory service only works with non-Java based phones. Any Java based phone will display duplicate directories for the following:
    - Missed
    - Received
    - Placed

Before You Begin

To use a Cisco Unified Communications Manager directory as an external directory source for Cisco Unified CME phones, the Cisco Unified Communications Manager must be made aware of the phones. You must list the MAC addresses of the Cisco Unified CME phones in the Cisco Unified Communications Manager and reset the phones from the Cisco Unified Communications Manager. It is not necessary for you to assign ephone-dns to the phones or for the phones to register with Cisco Unified Communications Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **url directories** *url*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**url directories** *url* **Example:** `Router(config-telephony)# url directories http://10.0.0.11/localdirectory`	Associates a URL with the programmable Directories feature button on supported Cisco Unified IP phones in Cisco Unified CME. • Provisioning the directories URL to select an external directory resource disables the Cisco Unified CME local directory service. • Operation of these services is determined by the Cisco Unified IP phone capabilities and the content of the specified URL.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Exits configuration mode and enters privileged EXEC mode.

Called-Name Display

To enable called-name display, perform the following steps.

Restriction

- The **service dnis overlay** command can only be used to configure overlaid ephone-dns.

Before You Begin

- For directory numbers other than overlaid directory numbers—To display a name in the called-name display, the name to be displayed must be defined in the local directory. See Add an Entry to a Local Directory on SCCP Phone, on page 663.
- For overlaid directory numbers—To display a name in the called-name display for a directory number that is in a set of overlaid directory numbers, the name to be displayed must be defined. See Define a Name for a Directory Number on SCCP Phone, on page 662.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **service dnis dir-lookup**
5. **service dnis overlay**
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	**telephony-service** **Example:** `Router(config)#`	Enters telephony-service configuration mode.
Step 4	**service dnis dir-lookup** **Example:** `Router(config-telephony)# service dnis dir-lookup`	Specifies that incoming calls to a called number should display the name that was defined for this directory number with the **directory entry** command. • If the **service dnis dir-lookup** and **service dnis overlay** commands are both used in one configuration, the **service dnis dir-lookup** command takes precedence.
Step 5	**service dnis overlay** **Example:** `Router(config-telephony)# service dnis overlay`	(For overlaid directory numbers only.) Specifies that incoming calls to a called number should display the name that was defined for this directory number with the **name** command. **Note** If the **service dnis dir-lookup** and **service dnis overlay** commands are both used in one configuration, the **service dnis dir-lookup** command takes precedence.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify Called-Name Display

Step 1 Use the **show running-config** command to verify your configuration. Called-name display is shown in the telephony-service part of the output.

Example:

```
Router# show running-config
telephony-service
 service dnis overlay
```

Step 2 Use the **show telephony-service directory-entry** command to display current directory entries.

Example:

```
Router# show telephony-service directory-entry

 directory entry 1 5550341 name doctor1
 directory entry 2 5550772 name doctor1
 directory entry 3 5550263 name doctor3
```

Step 3 Use the **show telephony-service ephone-dn** command to verify that you have used at least one wildcard (period or .) in the ephone-dn primary or secondary number or to verify that you have entered a name for the number.

Example:

```
Router# show telephony-service ephone-dn

ephone-dn 2
 number 5002 secondary 200.
 name catalogN
 huntstop
 call-forward noan 5001 timeout 8
```

Step 4 Use the **show ephone overlay** command to verify the contents of overlaid ephone-dn sets.

Example:

```
Router# show ephone overlay

ephone-1 Mac:0007.0EA6.353A TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0

IP:10.2.225.205 52486 Telecaster 7960  keepalive 2771 max_line 6
button 1: dn 11 number 60011 CH1 IDLE      overlay
button 2: dn 17 number 60017 CH1 IDLE      overlay
button 3: dn 24 number 60024 CH1 IDLE      overlay
button 4: dn 30 number 60030 CH1 IDLE      overlay
button 5: dn 36 number 60036 CH1 IDLE      CH2 IDLE      overlay
button 6: dn 39 number 60039 CH1 IDLE      CH2 IDLE      overlay
overlay 1: 11(60011) 12(60012) 13(60013) 14(60014) 15(60015) 16(60016)
overlay 2: 17(60017) 18(60018) 19(60019) 20(60020) 21(60021) 22(60022)
overlay 3: 23(60023) 24(60024) 25(60025) 26(60026) 27(60027) 28(60028)
overlay 4: 29(60029) 30(60030) 31(60031) 32(60032) 33(60033) 34(60034)
overlay 5: 35(60035) 36(60036) 37(60037)
overlay 6: 38(60038) 39(60039) 40(60040
```

Define a Name for a Directory Number on SIP Phone

To define name for a directory number on a SIP phone, perform the following steps.

Before You Begin

- Cisco CME 3.4 or a later version.
- Directory number for which you are defining a name must already have a number assigned by using the **number (voice register dn)** command. For configuration information, see Create Directory Numbers for SIP Phones, on page 263.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **name** *name*
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 register dn** *dn-tag* **Example:** `Router(config-register-global)# voice register dn 17`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI).

Step 4	**name** *name*
	
	Example:
	`Router(config-register-dn)# name Smith, John`
	or
	`Router(config-register-dn)# name John Smith`
		Associates a name with a directory number in Cisco Unified CME and provides caller ID for calls originating from a SIP phone.
		• Name must follow the order specified by using the **directory (telephony-service)** command.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure External Directory Service on SIP Service

To enable an external directory resource on supported Cisco Unified IP phones and disable local directory services on those same phones, perform the following steps.

Restriction

- Provisioning of the directory URL to select an external directory resource disables the Cisco Unified CME local directory service.
- Supported only on Cisco Unified IP Phone 7960s and 7960Gs and Cisco Unified IP Phone 7940s and 7940Gs.

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **url directory** *url*
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.

	Command or Action	Purpose
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**url directory** *url* **Example:** `Router(config-register-global)# url directory http://10.0.0.11/localdirectory`	Associates a URL with the programmable Directories feature button on supported Cisco Unified IP phones in Cisco Unified CME. • Provisioning the directory URL to select an external directory resource disables the Cisco Unified CME local directory service. • Operation of these services is determined by the Cisco Unified IP phone capabilities and the content of the specified URL.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Verify Directory Services

To verify the configuration for local directory services, perform the following steps.

Step 1 **show running-config**

This command displays the running configuration. Directory configuration commands are listed in the telephony-service portion of the output.

Example:

```
Router# show running-config
.
.
.
timeout busy 10
timeout ringing 100
caller-id name-only: enable
system message XYZ Company
web admin system name admin1 password admin1
web admin customer name Customer
edit DN through Web:  enabled.
edit TIME through web:  enabled.
Log (table parameters):
     max-size: 150
     retain-timer: 15
create cnf-files version-stamp Jan 01 2002 00:00:00
transfer-system full-consult
multicast moh 239.12.20.123 port 2000
fxo hook-flash
```

```
local directory service: enabled.
```

Step 2 **show telephony-service**
This command displays only the telephony-service configuration information.

Step 3 Use the **show telephony-service directory-entry** command to display the entries made using the **directory entry** command.

Configuration Examples for Directory Services

Example for Configuring Local Directory

The following example defines the naming order for the local directory on IP phones served by the Cisco Unified CME router:

```
telephony-service
directory last-name-first
```

The following example creates a directory of three telephone listings:

```
telephony-service
directory entry 1 14045550111 name Sales
directory entry 2 13125550122 name Marketing
directory entry 3 12135550144 name Support Center
```

The following example disables the local directory on IP phones served by the Cisco Unified CME router:

```
telephony-service
no service local-directory
```

Example for Configuring Called-Name Display

This section contains the following examples:

Example for Called-Name Display for Voice Hunt Group

The following is an example of a voice hunt group configuration, where the CLI command **service dnis dir-lookup** allows the directory entry names to be displayed on the IP phones when a call is placed to a number declared using the CLI command **directory entry**. In this example, the pilot umber is configured as 11… This means that the user can dial the numbers 1100 to 1199. When the user dials 1111, the directory name dept1 is displayed for the directory numbers 2001, 2002, and 2003. If user dials 1155, then the directory name dept2 is displayed and if user dials 5500, then the directory name dept3 is displayed for the directory numbers 2001, 2002, and 2003.

```
telephony-service
 service dnis dir-lookup
 directory entry 1 1111 name dept1
 directory entry 2 1155 name dept2
```

```
 directory entry 3 5500 name dept3

voice hunt-group 1 sequential
pilot 11..
list 2001, 2002, 2003
final 8888
timeout 10
```

Example for Configuring First Ephone-dn in the Overlay Set

The following example shows a configuration for three phones that use the same set of overlaid ephone-dns for each phone's button 1.

```
telephony-service
 service dnis overlay

ephone-dn 1
 number 18005550100

ephone-dn 2
 name department1
 number 18005550101

ephone-dn 3
 name department2
 number 18005550102

ephone 1
 button 1o1,2,3

ephone 2
 button 1o1,2,3

ephone 3
 button 1o1,2,3
```

The default display for all three phones is the number of the first ephone-dn listed in the overlay set (18005550100). A call is made to the first ephone-dn (18005550100), and the caller ID (for example, 4085550123) is displayed on all three phones. The user for phone 1 answers the call. The caller ID (4085550123) remains displayed on phone 1, and the displays on phone 2 and phone 3 return to the default display (18005550100). A call to the next ephone-dn is made. The default display on phone 2 and phone 3 is replaced with the called ephone-dn's name (18005550101).

Example for Configuring Directory Name for an Overlaid Ephone-dn Set

The following is an example of a configuration of overlaid ephone-dns that uses wildcards in the secondary numbers for the ephone-dns. The wildcards allow you to control the display according to the number that was dialed. The example is for a medical answering service with three IP phones that accept calls for nine doctors on one button. When a call to 5550001 rings on button 1 on ephone 1 through ephone 3, "doctor1" is displayed on all three ephones.

```
telephony-service
 service dnis dir-lookup

 directory entry 1 5550001 name doctor1
 directory entry 2 5550002 name doctor2
 directory entry 3 5550003 name doctor3
 directory entry 4 5550010 name doctor4
 directory entry 5 5550011 name doctor5
 directory entry 6 5550012 name doctor6

 directory entry 7 5550020 name doctor7
```

```
 directory entry 8 5550021 name doctor8
 directory entry 9 5550022 name doctor9

ephone-dn 1
 number 5500 secondary 555000.

ephone-dn 2
 number 5501 secondary 555001.

ephone-dn 3
 number 5502 secondary 555002.

ephone 1
 button 1o1,2,3
 mac-address 1111.1111.1111

ephone 2
 button 1o1,2,3
 mac-address 2222.2222.2222

ephone 3
 button 1o1,2,3
 mac-address 3333.3333.3333
```

For more information about making directory entries, see Local Directory, on page 659 . For more information about overlaid ephone-dns, see Call Coverage Features, on page 1239.

Example for Configuring Directory Name for a Hunt Group with Overlaid Ephone-dns

The following example shows a hunt-group configuration for a medical answering service with two phones and four doctors. Each phone has two buttons, and each button is assigned two doctors' numbers. When a patient calls 5550341, Cisco Unified CME matches the hunt-group pilot secondary number (555....), rings button 1 on one of the two phones, and displays "doctor1."

```
telephony-service
 service dnis dir-lookup
 max-redirect 20
 directory entry 1 5550341 name doctor1
 directory entry 2 5550772 name doctor1
 directory entry 3 5550263 name doctor3
 directory entry 4 5550150 name doctor4

ephone-dn 1
 number 1001

ephone-dn 2
 number 1002

ephone-dn 3
 number 1003

ephone-dn 4
 number 104

ephone 1
 button 1o1,2
 button 2o3,4
 mac-address 1111.1111.1111

ephone 2
 button 1o1,2
 button 2o3,4
 mac-address 2222.2222.2222


ephone-hunt 1 peer
 pilot 5100 secondary 555....
 list 1001, 1002, 1003, 1004
```

```
 final number 5556000
 hops 5
 preference 1
 timeout 20
 no-reg
```

For more information about hunt-group behavior, see Call Coverage Features, on page 1239. Note that wildcards are used only in secondary numbers and cannot be used with primary numbers. For more information about making directory entries, see Call Coverage Features, on page 1239. For more information about overlaid ephone-dns, see Call Coverage Features, on page 1239.

Example for Configuring Directory Name for Non-Overlaid Ephone-dns

The following is a configuration for three IP phones, each with two buttons. Button 1 receives calls from doctor1, doctor2, and doctor3, and button 2 receives calls from doctor4, doctor5, and doctor6.

```
telephony-service
 service dnis dir-lookup
 directory entry 1 5550001 name doctor1
 directory entry 2 5550002 name doctor2
 directory entry 3 5550003 name doctor3
 directory entry 4 5550010 name doctor4
 directory entry 5 5550011 name doctor5 directory entry 6 5550012 name doctor6

ephone-dn 1
 number 1001 secondary 555000.

ephone-dn 2
 number 1002 secondary 555001.

ephone 1
 button 1:1
 button 2:2
 mac-address 1111.1111.1111

ephone 2
 button 1:1
 button 2:2
 mac-address 2222.2222.2222

ephone 3
 button 1:1
 button 2:2
 mac-address 3333.3333.3333
```

For more information about making directory entries, see Local Directory, on page 659.

Example for Configuring Ephone-dn Name for Overlaid Ephone-dns

The following example shows three phones that have button 1 assigned to pick up three 800 numbers for three different catalogs.

The default display for all four phones is the number of the first ephone-dn listed in the overlay set (18005550000). A call is made to the first ephone-dn (18005550000), and the caller ID (for example, 4085550123) is displayed on all phones. The user for phone 1 answers the call. The caller ID (4085550123) remains displayed on phone 1, and the displays on phone 2 and phone 3 return to the default display (18005550000). A call to the second ephone-dn (18005550001) is made. The default display on phone 2 and phone 3 is replaced with the called ephone-dn's name (catalog1) and number (18005550001).

```
telephony-service
 service dnis overlay
```

```
ephone-dn 1
 number 18005550000

ephone-dn 2
 name catalog1
 number 18005550001

ephone-dn 3
 name catalog2
 number 18005550002

ephone-dn 4
 name catalog3
 number 18005550003

ephone 1
 button 1o1,2,3,4

ephone 2
 button 1o1,2,3,4

ephone 3
 button 1o1,2,3,4
```

For more information about overlaid ephone-dns, see Call Coverage Features, on page 1239.

Feature Information for Directory Services

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

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

Table 41: Feature Information for Directory Services

Feature Name	Unified CME Version	Feature Information
Service Local Directory	12.0	The CLI command for accessing local directory service was enhanced to configure username and password, as **service local-directory authenticate username password** .
Directory Search	7.0/4.3	Number of entries supported in a search results list was increased from 32 to 240 when using directory search.

Feature Name	Unified CME Version	Feature Information
Called-Name Display	12.0	Support for Called-Name Display on phones configured under voice hunt group.
	3.2	Called-Name Display was introduced.
Local Directory Service External Directory Service	4.0(2)	Added support for transferring a call directly to a selected number listed in the directory. If directory transfer is not supported, the user must press Transfer and then use the keypad to manually enter the number of the monitored line to transfer the incoming call.
	3.4	Added support of directory services for SIP phones directly connected in Cisco Unified CME.
	3.0	The ability to add local directory entries in addition to those that are automatically added from phone configurations was introduced. Authentication for local directory display was introduced.
	2.1	The ability to block the display of the local directory on phones was introduced.
	2.0	The specification of name format in the local directory was introduced.

CHAPTER 19

Do Not Disturb

Information About Do Not Disturb

Do Not Disturb on SCCP Phone

The Do Not Disturb (DND) feature allows phone users to disable audible ringing for incoming calls. When DND is enabled, incoming calls do not ring on the phone, however there is visual alerting and the call information displays, and a call can be answered if desired. When a local IP phone calls another local IP phone that is in the DND state, the message “Ring out DND” displays on the calling phone indicating that the target phone is in the DND state.

Phone users can toggle DND on and off by using the DND softkey in the idle or ringing call states. A SSCP phone user can toggle DND on or off in the ringing state only if DND in not already active on the phone. If DND is already active when a new call comes in, the SCCP phone user cannot change the DND state by pressing the DND softkey.

If an SSCP phone user toggles DND on during an incoming call, the DND state remains active for the current call only. If a SIP phone user toggles DND on during an incoming call, the DND state remains active during the current call and for all future calls until the user explicitly toggles DND off.

Pressing the DND softkey during an incoming call forwards the call to the call-forward no answer destination if Call Forward No Answer is enabled. If Call Forward is not enabled, pressing the DND softkey disables audible ringing and visual alerting, but the call information is visible on the phone display.

In Cisco CME 3.2.1 and later versions, DND can be blocked from phones with the feature-ring function. A feature ring is a triple-pulse ring, a type of ring cadence in addition to internal call and external call ring cadences. For example, an internal call in the United States rings for 2 seconds on and 4 seconds off (single-pulse ring), and an external call rings for 0.4 seconds on, 0.2 seconds off, 0.4 seconds on, and 0.2 seconds off (double-pulse ring).

The triple-pulse ring is used as an audio identifier for phone users. For example, each salesperson in a sales department could have an IP phone with a button sharing the same set of ephone-dns with the sales staff and another button for their private line for preferred customers. To help a salesperson identify an incoming call to his or her private line, the private line can be configured with the feature-ring function. You can disable the DND function on feature-ring lines. In the preceding example, salespeople could activate DND on their phones and still hear calls to their private lines.

Do Not Disturb on SIP Phone

In Cisco Unified CME 7.1 and later versions, the Do Not Disturb (DND) feature for SIP phones prevents incoming calls from audibly ringing a phone. When DND is enabled, the phone flashes an alert to visually indicate an incoming call instead of ringing and the call can be answered if desired. The message "Do Not Disturb is active" displays on the phone and calls are logged to the Missed Calls directory.

In versions earlier than Cisco Unified CME 7.1, the DND feature blocks incoming calls to a SIP phone with a busy tone. Cisco Unified CME rejects calls to all lines on the phone and plays a busy tone to the caller. Received calls are not logged to the Missed Calls directory on the phone.

DND applies to all lines on the phone. If DND and Call Forward All are both enabled on a phone, Call Forward All takes precedence on incoming calls.

You must enable DND for a SIP phone through Cisco Unified CME. The DND softkey displays by default on supported SIP phones in both the Ringing and idle states. You can remove or change the order of this softkey using a voice register template.

A phone user can toggle DND on and off at the phone by using the DND softkey. If a SIP phone user activates DND during an incoming call, the DND state remains active during the current call and for all future calls until the user explicitly toggles DND off.

If a phone user toggles DND on or off at the phone, Cisco Unified CME restores the DND state after the phone resets or restarts, if you save the running configuration before Cisco Unified CME reboots.

For configuration information, see Configure Do Not Disturb on SIP Phones, on page 683.

Table 42: DND Feature Comparison for SIP Phones, on page 680 compares the DND configuration for SIP phones with different phone load versions:

Table 42: DND Feature Comparison for SIP Phones

	Cisco Unified IP Phone 7911, 7941, 7961, 7970, or 7971 with 8.3 Phone Load	**Cisco Unified IP Phone 7911, 7941, 7961, 7970, or 7971 with 8.2 Phone Load or Cisco Unified IP Phone 7940 or 7960**
DND support	**dnd** command in voice register pool mode	**dnd** command in voice register pool mode
DND softkey display	**softkey idle** and **softkey ringIn** command in voice register template mode	**dnd-control** command in voice register template mode
Behavior when configured	Ringer is turned off for incoming calls. Visual alerting is provided.	Call is rejected and busy tone is played to the caller.

Configure Do Not Disturb

Blocking Do Not Disturb on SCCP Phone

To block DND on phones that have buttons configured for feature ringing, perform the following steps. DND is enabled by using the DND softkey on Cisco Unified IP phones that support softkeys.

Restriction

- Phone users cannot enable DND for a shared line in a hunt group. The softkey displays in the idle and ringing states but does not enable DND for shared lines in hunt groups.

Before You Begin

- Cisco Unified 3.2.1 or a later version.
- Phone line must be configured for feature ring with the button f command.
- Call-forwarding no-answer must be set for a phone to use DND to forward calls. For configuration information, see Configure Call Transfer and Forwarding, on page 1178. No other configuration is necessary for basic DND.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **no dnd feature-ring**
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** *phone-tag*	Enters ephone configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# ephone 10`	• *phone-tag*—Unique sequence number that identifies the ephone to be configured.
Step 4	**no dnd feature-ring** **Example:** `Router(config-ephone)# no dnd feature-ring`	Enables ringing on phone buttons configured for feature ring when the phone is in DND mode.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

In the following configuration example, when DND is activated on ephone 1 and ephone 2, button 1 will ring, but button 2 will not.

```
ephone-dn 1
 number 1001

ephone-dn 2
 number 1002

ephone-dn 10
 number 1110
 preference 0
 no huntstop

ephone-dn 11
 number 1111
 preference 1

ephone 1
 button 1f1
 button 2o10,11
 no dnd feature-ring

ephone 2
 button 1f2
 button 2o10,11
 no dnd feature-ring
```

Verify Do Not Disturb on SCCP Phones

show ephone dnd

Use this command to display a list of SCCP phones that have DND enabled.

```
Router# show ephone dnd

ephone-1 Mac:0007.0EA6.353A TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:1.2.205.205 52486 Telecaster 7960  keepalive 2729 max_line 6 DnD
button 1: dn 11 number 60011 CH1 IDLE
```

Configure Do Not Disturb on SIP Phones

To enable the Do Not Disturb (DND) feature on a SIP phone, perform the following steps.

Restriction

- In versions earlier than Cisco Unified CME 7.1, you enable the DND softkey on SIP phones by using the **dnd-control** command.
- If you enable DND on the phone and remove the DND softkey, the user cannot toggle DND off at the phone.

Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE

- For SIP phones using firmware 8.3 or a later version, the DND feature prevents calls from ringing; it does not block calls or play a busy tone to the caller.
- If DND is disabled by a phone user, it is not enabled after the phone resets or restarts. DND must be enabled both in Cisco Unified CME*and* by using the DND softkey on the phone.

Before You Begin

- Cisco CME 3.4 or a later version.
- Cisco Unified CME 7.1 or a later version to use the DND softkey.
- Call-forwarding busy must be set for a SIP IP phone to use DND to forward calls. For configuration information, see Configure Call Transfer and Forwarding, on page 1178.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **softkeys idle** {[**Cfwdall**] [**DND**] [**Gpickup**] [**Newcall**] [**Pickup**] [**Redial**]}
5. **softkeys ringIn** [**Answer**] [**DND**]
6. **exit**
7. **voice register pool** *phone-tag*
8. **dnd**
9. **template** *template-tag*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.
Step 4	**softkeys idle** {[**Cfwdall**] [**DND**] [**Gpickup**] [**Newcall**] [**Pickup**] [**Redial**]} **Example:** `Router(config-register-temp)# softkeys idle`	Modifies the order and type of softkeys that display on a SIP phone during the idle call state.
Step 5	**softkeys ringIn** [**Answer**] [**DND**] **Example:** `Router(config-register-temp)# softkeys ringin dnd answer`	Modifies the order and type of softkeys that display on a SIP phone during the ringing call state.
Step 6	**exit** **Example:** `Router(config-register-temp)# exit`	Exits ephone-template configuration mode.
Step 7	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 1`	Enters voice register pool configuration mode to set parameters for the SIP phone.
Step 8	**dnd** **Example:** `Router(config-register-pool)# dnd`	Enables DND on the phone. • If Call Forward No Answer is not configured for the extension, pressing the DND softkey mutes the ringer for incoming calls.
Step 9	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3, on page 684.

	Command or Action	Purpose
Step 10	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

The following example shows DND is enabled on phone 130, and the DND softkey is modified in template 6, which is assigned to the phone:

```
voice register template  6
 softkeys idle  Gpickup Pickup DND Redial
 softkeys ringIn  DND Answer
!
voice register pool  130
 id mac 001A.A11B.500E
 type 7941
 number 1 dn 30
 template 6
 dnd
```

Where to Go Next

Agent Status Control for Ephone Hunt Groups and Cisco Unified CME B-ACD

Ephone hunt group agents can control their ready/not-ready status (their ability to receive calls) using the DND function or the HLog function of their phones. When they use the DND softkey, they do not receive calls on any extension on their phones. When they use the HLog softkey, they do not receive calls on hunt group extensions, but they do receive calls on other extensions. For more information on agent status control and the HLog function, see Call Coverage Features, on page 1239.

Call Forwarding

To use the DND softkey to forward calls, enable call-forwarding no-answer for SCCP phones or call-forward busy for SIP IP phones. See Configure Call Transfer and Forwarding, on page 1178.

Feature Access Codes (FACs)

DND can be activated and deactivated using a feature access code (FAC) instead of the DND softkey when standard or custom FACs are enabled. The following is the standard FAC for DND:

- DND **7

See Feature Access Codes, on page 757.

Softkey Display

You can remove or change the position of the DND softkey. See Customize Softkeys, on page 925.

Feature Information for Do Not Disturb

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

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

Table 43: Feature Information for Do Not Disturb

Feature Name	Cisco Unified CME Version	Feature Information
Do Not Disturb	7.1	Enhanced DND support on SIP phones to allow incoming calls to visually flash an alert.
	3.4	Added support for Do-not-disturb (DND) softkey on SIP phones.
	3.2.1	DND bypass for feature-ring phones was introduced.
	3.2	DND was introduced.

CHAPTER 20

Enhanced 911 Services

Prerequisites for Enhanced 911 Services

- SCCP or SIP phones must be registered to Cisco Unified CME.
- At least one CAMA or ISDN trunk must be configured from Cisco Unified CME 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 CME has an FXS, FXO, SIP, or H.323 trunk interface configured.

Cisco Unified CME

- Cisco Unified CME 4.2 or a later version.

Cisco Unified CME in SRST Fallback Mode

- Cisco Unified CME 4.1 or a later version, configured in SRST fallback mode. See SRST Fallback Mode, on page 1539.

Note For information about configuring ephones, ephone-dns, voice register pools, and voice register dns, see Configure Phones to Make Basic Call, on page 315.

Restrictions for Enhanced 911 Services

- Enhanced 911 Services for Cisco Unified CME 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 CME.
- Cisco Emergency Responder does not have access to any updates made to the emergency call history table when remote Cisco Unified IP phones are in SRST fallback mode. Therefore, if the PSAP calls back after the IP phones register back to Cisco Unified Communications Manager, Cisco Emergency Responder has no history of those calls. As a result, those calls are not routed to the original 911 caller. Instead, the calls are routed to the default destination that is configured on Cisco Emergency Responder for the corresponding ELIN.
- For Cisco Unified Wireless 7920 and 7921 IP phones, a caller's location can only be determined by the static information configured by the system administrator. For more information, see Precautions for Mobile Phones, on page 693.
- 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 Overview of Enhanced 911 Services, on page 688.
- Using ELINs for multiple purposes can result in unexpected interactions with existing Cisco Unified CME features. These multiple uses of an ELIN can include configuring an ELIN for use as an actual phone number (ephone-dn, voice register dn, or FXS destination-pattern), a Call Pickup number, or an alias rerouting number. For more information, see Multiple Usages of an ELIN, on page 696.
- Your configuration of Enhanced 911 Services can interact with existing Cisco Unified CME features and cause unexpected behavior. For a complete description of interactions between Enhanced 911 Services and existing Cisco Unified CME features, see Interactions with Existing Cisco Unified CME Features, on page 695.

Information About Enhanced 911 Services

Overview of Enhanced 911 Services

Enhanced 911 Services enable 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 CME 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 then had 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 CME. 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 Cisco IOS **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 CME 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. You can use this designated callback number if 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 desired 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.

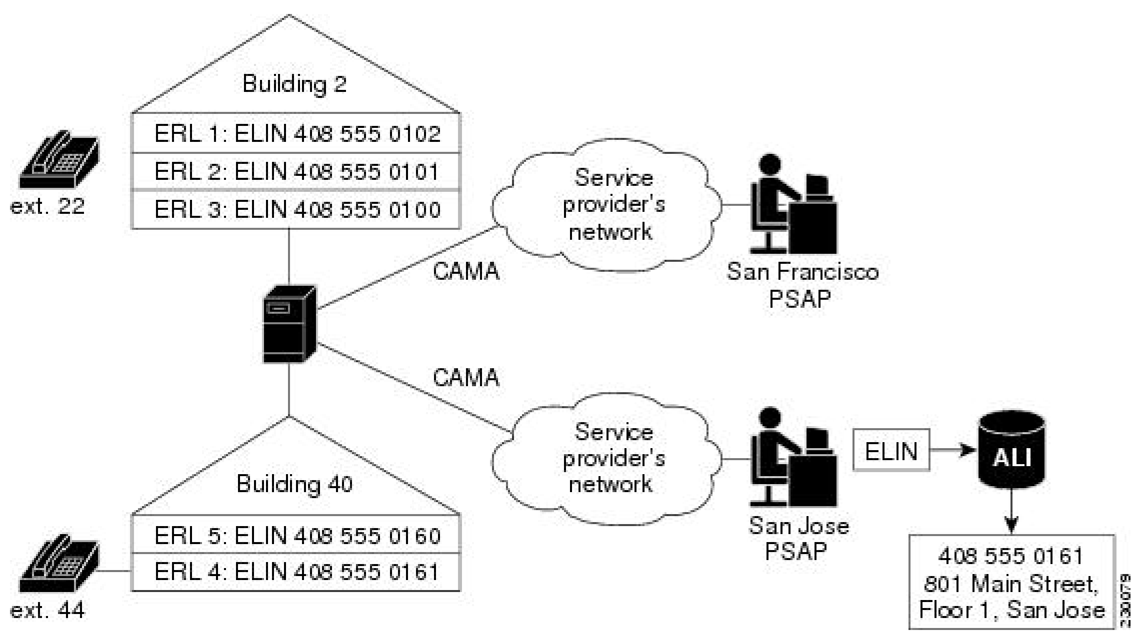
Note

- If a caller's IP address does not match any location in its dial-peers 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 24: Implementation of Enhanced 911 for Cisco Unified CME, on page 690 shows 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. 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 are routed based on matching the destination number configured for the outgoing dial peers.

Figure 24: Implementation of Enhanced 911 for Cisco Unified CME



Call Processing for E911 Services

When a 911 call is received by Cisco Unified CME, the initial call processing is the same as for any other call. Cisco Unified CME 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 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

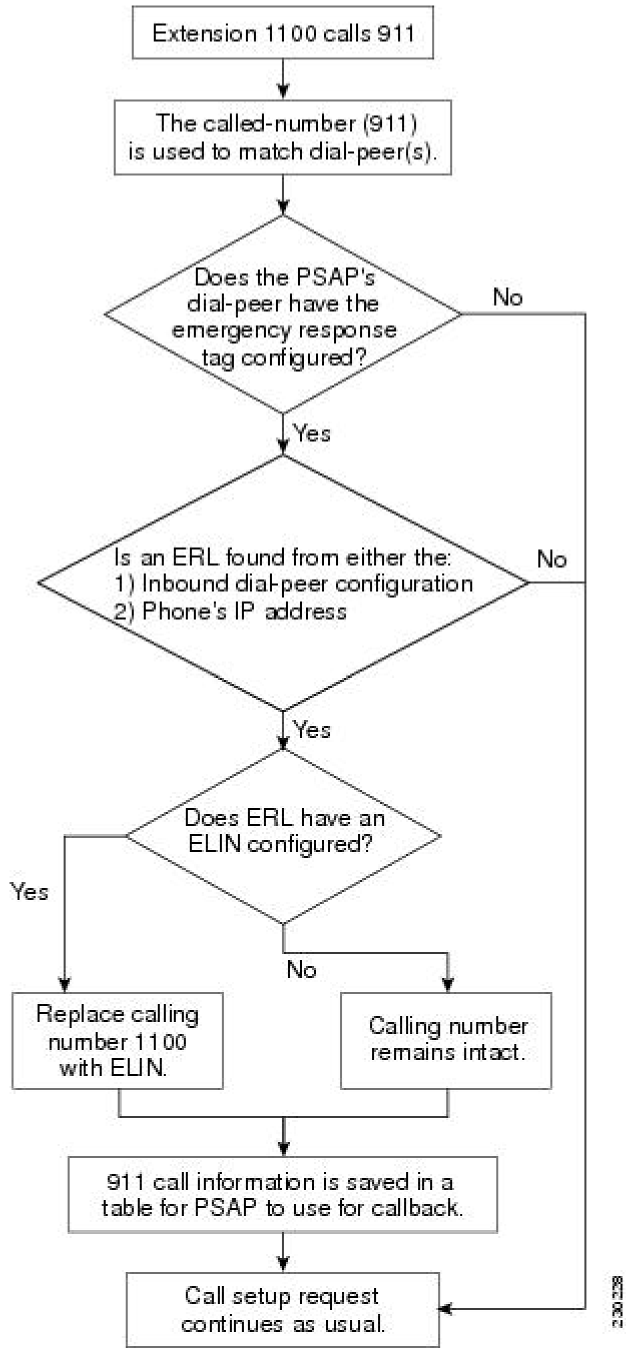
The Last Caller table contains this information for the most recent emergency callers from each ERL. A caller's information is purged from the table when the specified expiry time has passed after the call was originated. If no time limit is specified, the default expiry time is three hours.

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 25: Processing a 911 Call, on page 692 summarizes the procedure for processing a 911 call.

Figure 25: Processing a 911 Call



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 Customize E911 Settings, on page 710. 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.

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. IP phones should not be used 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 (in other words, their 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.

Plan Your Implementation of Enhanced 911 Services

Before you configure Enhanced 911 Services for Cisco Unified CME:

Step 1 Make a list of your sites that are serviced by Cisco Unified CME, and the PSAPs serving each site.
Be aware that you must use a CAMA/PRI interface to connect to each PSAP. Table 44: List of Sites and PSAPs, on page 694 shows an example of the information that you need to gather.

Table 44: List of Sites and PSAPs

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 need to 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 45: ERL Calculation, on page 694 shows an example.

Table 45: 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 ERLs to phones.
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 46: Definitions of ERL, Description, IP Subnets, and ELIN, on page 694 shows an example.

Table 46: Definitions of ERL, Description, IP Subnets, and ELIN

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

ERL Number	Description	IP Address Assignment	ELIN
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 or 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 SCCP phones 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:
    - Dial-peer configuration
    - Ephone configuration (SCCP phones)
    - Voice register pool configuration (SIP phones)

Table 47: Explicit ERL Assignment Per Phone, on page 695 shows examples of each of these options.

Table 47: Explicit ERL Assignment Per Phone

Phone Configuration	ERL
Dial-peer voice 213 pots	3
Dial-peer voice 214 voip	4
Ephone 100	3
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 CME Features

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

Note Your version of Cisco Unified CME may not support all of these features.

Multiple Usages of an ELIN

Note We recommend that you do not use ELINs for any other purpose because of possible unexpected interactions with existing Cisco Unified CME 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-expansion—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 CME environment performs a semi attended 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.

Caution 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.

Configure Enhanced 911 Services

Configure the Emergency Response Location

Perform this procedure to create the ERL. The ERL defines an area that allows emergency teams to quickly locate a caller.

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.

Before You Begin

- Cisco Unified CME 4.1 or a later version.

- The **address** and **name** commands are supported in Cisco Unified CME 4.2 and later versions.
- Plan your 911 configuration as described in Plan Your Implementation of Enhanced 911 Services, on page 693

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 14085550100`	(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 comma-separated string used for the automatic location identification (ALI) database upload of the caller's address. • String must conform to the record format that is required by the service provider. The string maximum is 247 characters.

	Command or Action	Purpose
		• 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. • This command is supported in Cisco Unified CME 4.2 and later versions.
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. • This command is supported in Cisco Unified CME 4.2 and later versions.
Step 7	**end** **Example:** `Router(cfg-emrgncy-resp-location)# end`	Returns to privileged EXEC mode.

Configure 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.

Before You Begin

- Cisco Unified CME 4.2 or a later version
- Define your ERLs as described in Configure the Emergency Response Location, on page 698.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice emergency response zone** *tag*
4. **location** *location-tag* [**priority** *number*]
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. • *tag*—Range is 1-100.
Step 4	**location** *location-tag* [**priority** *number*] **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. • *number*—(optional) Ranks the location in the zone list. Range is 1-100, with 1 being the highest priority. • Repeat this command for each location included in the zone.
Step 5	**end** **Example:** `Router(cfg-emrgncy-resp-zone)# end`	Returns to privileged EXEC mode.

Configure 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 Plan Your Implementation of Enhanced 911 Services, on page 693, use one of the following procedures:

- If you decided to not use zones, see Configure Dial Peers for Emergency Calls, on page 701.
- If you decided to use zones, see Configure Dial Peers for Emergency Response Zones, on page 703.

Configure 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.

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.
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.

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

Configure Dial Peers for Emergency Response Zones

You can selectively route a 911 call based on the ERL by assigning different zones to dial peers. The **emergency response zone** command identifies the dial peer that routes the 911 call and the voice interface to use. Only ERLs that are defined in the zone can be routed on the dial peer. Callers dialing the same emergency number are routed to different voice interfaces based on the zone of the ERL.

Before You Begin

- Cisco Unified CME 4.2 or a later version
- Define your ERLs and emergency response zones as described in:
    - Configure the Emergency Response Location, on page 698
    - Configure Locations under Emergency Response Zones, on page 700

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.

	Command or Action	Purpose
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. • *tag*—Points to an existing configured zone. Range is 1-100.
Step 7	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Configure 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 chapter *Configuring Voice Ports* in the Cisco Voice, Video, and Fax Configuration Guide.
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.

Assign ERLs to Phones

You must specify an ERL for each phone. The type of phones that you have determines which of the following tasks you use to associate an ERL with your phones, as explained in *Step 7* in Plan Your Implementation of Enhanced 911 Services, on page 693.

- To create an IP subnet in the ERL that includes each phone's IP address, you must also configure each ERL to specify which phones are part of the ERL. See Assign an ERL to a Phone's IP Subnet, on page 706. You can optionally specify up to two different subnets.
- To assign an ERL to a SIP phone, you must specify the ERL in the voice register pool configuration. See Assign an ERL to a SIP Phone, on page 707.
- To assign an ERL to a SCCP phone, you must specify the ERL in the ephone configuration. See Assign an ERL to a SCCP Phone, on page 708.
- To assign an ERL to a phone's dial peer, you must specify the ERL in the dial-peer configuration. See Assign an ERL to a Dial Peer, on page 709.

Prerequisites for Assigning ERLs to Phones

Define your ERLs and emergency response zones as described in the Configure the Emergency Response Location, on page 698.

Assign an ERL to a Phone's IP Subnet

Use this procedure 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 that all IP phones in a specific subnet 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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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.

Assign an ERL to a SIP Phone

Perform this procedure if you chose to assign a specific ERL to a SIP phone instead of using the phone's IP address to match a subnet defined for an ERL. For more information about this decision, see *Step 7* in Plan Your Implementation of Enhanced 911 Services, on page 693.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *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	**voice register pool** *tag* **Example:** `Router(config)# voice register pool 8`	Enters voice register pool mode to define parameters for an individual voice register pool.
Step 4	**emergency response location** *tag* **Example:** `Router(config-register-pool)# emergency response location 12`	Assigns an ERL to a phone s voice register pool using an ERL s tag. • *tag*—Range is 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. • This command can also be configured in voice register template configuration mode and applied to one or more phones. The voice register pool configuration has priority over the voice register template configuration.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Assign an ERL to a SCCP Phone

Perform this procedure if you chose to assign an ERL to a SCCP phone instead of configuring an ERL to be associated with IP subnets. For more information about this decision, see *Step 7* in Plan Your Implementation of Enhanced 911 Services, on page 693.

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. • *tag*—Range is 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. • This command can also be configured in ephone-template configuration mode and applied to one or more phones. The ephone configuration has priority over the ephone-template configuration.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Assign 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 Plan Your Implementation of Enhanced 911 Services, on page 693.

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.

Customize E911 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]
```

Before You Begin

- Cisco Unified CME 4.2 or a later version

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.

	Command or Action	Purpose
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

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
```

Enable Call Detail Records

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
```

Verify E911 Configuration

New **show** commands are introduced to display E911 configuration or usage.

- 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
```

- 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
```

Troubleshooting Enhanced 911 Services

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

Example for Configuring Enhanced E911 Services with Cisco Unified CME 4.2

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
!
```

Example for Configuring Enhanced E911 Services with Cisco Unified CME 4.1 in SRST Fallback Mode

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
- An ephone
- A SI P phone

```
Router#show running-config

Building configuration...

Current configuration : 7557 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 logging console
!
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
!
!
telephony-service
srst mode auto-provision none
load 7960-7940 P00307020200
load 7970 TERM70.7-0-1-0s
load 7912 CP7912060101SCCP050429B.sbin
max-ephones 50
max-dn 190
ip source-address 10.20.20.3 port 2000
system message RM-SCCP-CME-SRST
max-conferences 8 gain -6
moh flash:music-on-hold.au
multicast moh 236.1.1.1 port 3000
transfer-system full-consult
transfer-pattern .....
transfer-pattern 911
!
!
ephone-dn  1  dual-line
number 31101
!
!
ephone-dn  2  dual-line
number 31201
!
!
ephone-dn  3  dual-line
number 31301
!
!
ephone-dn  100  dual-line
number 37101 secondary 37111
name 7960-sccp-1
!
!
ephone-dn  101  dual-line
number 37102
!
!
ephone-dn  102  dual-line
number 37103
!
!
ephone-dn  105
number 37201
!
!
ephone-dn  106  dual-line
number 37101
!
!
ephone-dn  107  dual-line
number 37302
!
!
ephone-dn  108  dual-line
number 37303
!
!
ephone-dn  110  dual-line
number 37401
!
!
ephone-dn  111  dual-line
number 37402
```

```
!
!
ephone  1
mac-address DCC0.1111.0001
type 7960
button  1:1
!
!
ephone  2
mac-address DCC0.1111.0002
type 7960
button  1:2
!
!
ephone  3
mac-address DCC0.1111.0003
type 7970
button  1:3
!
!
ephone  40
mac-address 0013.1AA6.7DCF
type 7960
button  1:100 2:101 3:102
!
!
ephone  41
mac-address 0012.0034.82CD
type 7912
button  1:105
!
!
ephone  42
mac-address 0014.F237.E000
 emergency response location 2
type 7940
button  1:107 2:108
!
!
ephone  43
mac-address 000F.90B0.BE0B
type 7960
button  1:110 2:111
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
!
end
```

Feature Information for Enhanced 911 Services

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

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

Table 48: Feature Information for Enhanced 911 Services

Feature Name	Cisco Unified CME Version	Feature Information
Enhanced 911 Services for Cisco Unified CME	4.2	• Assigns ERLs to zones to enable routing to the PSAP that is closest to the caller • Customizes 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 • Expands the E911 location information to include name and address • Uses templates to assign ERLs to a group of phones • Adds new permanent call detail records
Enhanced 911 Services	4.1	Enhanced 911 Services was introduced for Cisco Unified CME in SRST Fallback Mode.

CHAPTER 21

Extension Mobility

This chapter describes features in Cisco Unified Communications Manager Express (Cisco Unified CME) that provide support for phone mobility for end users.

Prerequisites for Configuring Extension Mobility

- Cisco Unified CME 4.2 or a later version.
- To use the web-based Cisco Unified CME GUI to configure personal speed dials on an Extension Mobility phone, Cisco Unified CME 4.2(1) or a later version must be installed.
- To use the phone user interface to configure personal speed dials directly on an Extension Mobility phone, Cisco Unified CME 4.3 or a later version must be installed.
- SIP phone support is available with Cisco Unified CME 8.6 or a later version.

Restrictions for Configuring Extension Mobility

- Extension Mobility on remote Cisco Unified CME routers is not supported; a phone user can log into any local Cisco Unified IP phone only.

Information About Configuring Extension Mobility

Extension Mobility

Extension Mobility in Cisco Unified CME 4.2 and later versions provides the benefit of phone mobility for end users.

A user login service allows phone users to temporarily access a physical phone other than their own phone and utilize their personal settings, such as directory number, speed-dial lists, and services, as if the phone is their own desk phone. The phone user can make and receive calls on that phone using the same personal directory number as is on their own desk phone.

Each Cisco Unified IP phone that is enabled for Extension Mobility is configured with a logout profile. This profile determines the default appearance of a phone that is enabled for Extension Mobility when there is no phone user logged into that phone. Minimally, the logout profile allows calls to emergency services such as 911. A single logout profile can be applied to multiple phones.

After a Cisco Unified IP phone that is enabled for Extension Mobility boots up, the Services feature button on the phone is configured with a login service URL hosted by Cisco Unified CME that points to the Extension Mobility Login page. No feature-button-specifc configuration is required to add Extension Assigner to the Services feature button. The option for Extension Mobility appears last in the list of options displayed when the phone user presses the Services feature button

A phone user logs in to a Cisco Unified IP phone that is enabled for Extension Mobility by pressing the Services button or a Unified CCX agent can log in using a Unified CCX Cisco Agent Desktop. User authentication and authorization is performed by Cisco Unified CME. If the login is successful, Cisco Unified CME retrieves the appropriate user profile, based on user name and password match, and replaces the phone's logout profile with the user profile.

After the phone user is logged in, the service URL points to a logout URL hosted by Cisco Unified CME to provide a logout prompt on the phone. Logging into a different device automatically closes the first session and start a new session on the new device. When a phone user is not logged in to any phone, incoming calls to the phone user's directory number are sent to the phone user's voice mailbox.

For button appearance, Extension Mobility associates directory numbers then speed-dial numbers in the logout profile or user profile to phone buttons. The sequence in which directory numbers are associated is based on line type and ring behavior as follows: first normal, then silent ring, beep ring, feature ring, monitor ring, and overlay, followed by speed dials. If the profile contains more numbers than there are buttons on the physical phone to which the profile is downloaded, the remaining numbers in the profile are ignored.

For configuration information, see Enable Extension Mobility, on page 730.

Personal Speed Dials on an Extension Mobility Phone

In Cisco Unified CME 4.2(1) and later versions, phone users can use the web-based GUI to set up personal speed dials on an Extension Mobility phone. Previously, the speed-dial configuration for a phone could only be done in Cisco Unified CME using Cisco IOS commands.

The same credential for logging on to an Extension Mobility phone is used to log into the Cisco Unified CME GUI. Any modifications made by using the phone user options in the GUI are applied to the phone user's user profile in Extension Mobility. Speed dial options in Cisco Unified CME GUI cannot be accessed from the System Administrator or Customer Administrator login screens.

For information about using the Cisco Unified CME GUI, see Cisco Unified CME Graphical User Interface User Guide.

The user name parameter of any authentication credential must be unique and cannot be the same as the user name for any other credential. Do not use the same value for a user name when you configure any two or more authentication credentials in Cisco Unified CME, such as the username for any Cisco United CME GUI account and the user name in a logout or user profile for Extension Mobility. For configuration information, see Enable the GUI, on page 525.

In Cisco Unified CME 4.3 and later versions, Extension Mobility users can configure their own speed-dial settings directly on the phone. Speed-dial settings are added or modified on the phone by using a menu available with the Services feature button. Any changes to the speed-dial settings made through the phone user interface are applied to the user's profile in Extension Mobility. For information about using the phone user interface on a Cisco Unified IP phone, see Cisco Unified IP Phone 7900 Series End-User Guides.

The phone user-interface is enabled by default on all phones with displays. You can disable the capability for an individual phone to prevent a phone user from accessing the interface. For configuration information, see Enable Phone User Interface for Configuring Speed-Dial and Fast-Dial, on page 978.

Cisco Unified CME Extension Mobility Enhancements

Enhancements to Extension Mobility in Cisco Unified CME 4.3 include the following:

- Configurable Automatic Logout
- Automatic Clear Call History

Automatic Logout

Cisco Unified CME 4.3 and later versions includes an Automatic Timeout feature for Extension Mobility. After an automatic logout is executed, Cisco Unified CME sends the logout profile to the phone and restarts the phone. After an automatic logout, Extension Mobility users can log in again.

You can configure up to three different times on a 24-hour clock for automatically logging out Extension Mobility users based on time-of-day. The system clock triggers an alarm at the specified time and the EM Manager in Cisco Unified CME logs outs every logged in Extension Mobility user in the system. If an Extension Mobility user is using the phone when automatic logout occurs, the user is logged out after the active call is completed.

For configuration information, see Configure Cisco Unified CME for Extension Mobility, on page 730.

Users log out from Extension Mobility by pressing the Services button and choosing Logout. If a user does not manually log out before leaving the phone, the phone is idle and the individual's user profile remains loaded on that phone. To automatically log out individual users from idle Extension Mobility phones, configure an idle-duration timer for Extension Mobility. The timer monitors the phone and if the specified maximum idle time is exceeded, the EM Manager logs out the user. The idle-duration timer is reset whenever the phone goes offhook.

For configuration information, see Configure a User Profile, on page 741.

Automatic Clear Call History

In Cisco Unified CME 4.3 and later versions, the EM manager in Cisco Unified CME issues commands to phones to clear call history whenever a user logs out of Extension Mobility. An HTTP GET/POST is sent between the Extension Mobility phone and the authentication server in Cisco Unified CME. The authentication server authorizes the request and the call history is cleared based on the result.

You can configure Cisco Unified CME to disable Automatic Clear Call History. For configuration information, see Configure Cisco Unified CME for Extension Mobility, on page 730.

Privacy on an Extension Mobility Phone

In Cisco Unified CME 4.3 and later versions, the Privacy feature enables phone users to block other users from seeing call information or barging into a call on a shared octo-line directory number. When a phone receives an incoming call on a shared octo-line, the user can make the call private by pressing the Privacy feature button, which toggles between on and off to allow the user to alter the privacy setting on their phone. The privacy state is applied to all new calls and current calls owned by the phone user.

For Extension Mobility phones, you can enable the privacy button in the user profile and logout profile. To enable the privacy button, see Configure a Logout Profile for an IP Phone, on page 733 and Configure a User Profile, on page 741.

For more information about Privacy, see Barge and Privacy, on page 1047.

Extension Mobility for SIP Phones Enhancement

Cisco Unified CME 8.6 enhances the Extension Mobility feature to allow support for SIP phones.

Extension Mobility allows you to access any EM enabled physical phone and utilize your own personal settings, such as directory numbers, speed-dials, after-hour personal identification number (PIN), and feature button layout, as if the phone is your own desk phone.

A user login service allows you to temporarily access a physical phone other than your own phone and utilize your personal settings, such as directory number, speed-dial lists, and services, as if the phone is your own desk phone.

The features of Extension Mobility for SIP phones is identical to SCCP phones, only the configuration procedure is different. For information on configuring Extension Mobility for SIP phones, see Configure Extension Mobility for SIP Phones, on page 738.

Note You can login to either an SCCP phone or a SIP phone with the same user profile.

Note Only the normal lines configured in your user profile are applied when you login to a SIP phone. Other lines such as overlay, monitor, and feature-ring lines are ignored.

Note Only Cfwdall, Confrn, DnD, Endcall, Hold, NewcallGroup Pickup, Park, Privacy, Redial, and Trnsfer feature buttons configured in your user profile will be applied when you login to a SIP phone. Other feature buttons will be ignored.

MIB Support for Extension Mobility in Cisco Unified SCCP IP Phones

In Cisco Unified CME 9.0 and later versions, new MIB objects are added to monitor Cisco Unified SCCP IP Extension Mobility (EM) phones. These enhancements allow the retrieval of the following information:

- user-profile tag for a Cisco Unified SCCP IP EM phone, when it is logged in
- logout-profile tag for a Cisco Unified SCCP IP EM phone
- DN and its type, and the overlay or call waiting numbers if applicable, for each user-profile
- DN and its type, and the overlay or call waiting numbers if applicable, for each logout-profile
- number of Cisco Unified SCCP IP phones configured as EM phones
- number of registered Cisco Unified SCCP IP EM phones

Table 49: MIB Variables and Object Identifiers for EM in Cisco Unfied SCCP IP Phones , on page 729 lists the MIB variables and object identifiers for retrieving the new MIB database.

Table 49: MIB Variables and Object Identifiers for EM in Cisco Unfied SCCP IP Phones

MIB Variables	Object identifiers
ccmeEMUserProfileTag	1.3.6.1.4.1.9.9.439.1.1.43.1.19
ccmeEMLogOutProfileTag	1.3.6.1.4.1.9.9.439.1.1.43.1.20
ccmeEMUserDirNumConfTable	1.3.6.1.4.1.9.9.439.1.1.68
ccmeEMUserDirNumConfEntry	1.3.6.1.4.1.9.9.439.1.1.68.1
ccmeEMUserDirNum	1.3.6.1.4.1.9.9.439.1.1.68.1.3
ccmeEMUserDirNumOverlay	1.3.6.1.4.1.9.9.439.1.1.68.1.4
ccmeEMLogoutDirNumConfTable	1.3.6.1.4.1.9.9.439.1.1.69
ccmeEMLogoutDirNumConfEntry	1.3.6.1.4.1.9.9.439.1.1.69.1
ccmeEMLogoutDirNum	1.3.6.1.4.1.9.9.439.1.1.69.1.3
ccmeEMLogoutDirNumOverlay	1.3.6.1.4.1.9.9.439.1.1.69.1.4
ccmeEMphoneTot	1.3.6.1.4.1.9.9.439.1.2.9
ccmeEMphoneTotRegistered	1.3.6.1.4.1.9.9.439.1.2.10

Table 50: Descriptions of MIB Variables for EM in Cisco Unfied SCCP IP Phones, on page 730 provides a description of each of the MIB variables for EM in Cisco Unified SCCP IP Phones.

Table 50: Descriptions of MIB Variables for EM in Cisco Unfied SCCP IP Phones

MIB Variables	Descriptions
ccmeEMUserProfileTag	User-profile tag for the EM phone
ccmeEMLogOutProfileTag	Logout-profile tag for the EM phone
ccmeEMUserDirNumConfTable	Table of entries for the EM phone's user profile
ccmeEMUserDirNumConfEntry	A user-profile entry for the EM phone
ccmeEMUserDirNum	A directory number for the user profile
ccmeEMUserDirNumOverlay	Number type for the user profile, including the overlay identifier
ccmeEMLogoutDirNumConfTable	Table of entries for the EM phone's logout profile
ccmeEMLogoutDirNumConfEntry	A logout entry for the EM phone
ccmeEMLogoutDirNum	A directory number for the logout profile
ccmeEMLogoutDirNumOverlay	Number type for the logout profile, including the overlay identifer
ccmeEMphoneTot	Total number of EM phones
ccmeEMphoneTotRegistered	Total number of registered EM phones

Extension mobility is supported in Cisco Unified CME but not in Cisco Unified SRST.

Enable Extension Mobility

Configure Cisco Unified CME for Extension Mobility

To configure Extension Mobility in Cisco Unified CME, perform the following steps.

Before You Begin

- For authentication server in Cisco Unified CME, Cisco Unified CME 4.3 or a later version.
- For Automatic Logout, Cisco Unified CME 4.3 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **telephony-service**
5. **url authentication** *url-address application-name password*
6. **service phone webAccess 0**
7. **authentication credential** *application-name password*
8. **em keep-history**
9. **em logout** *time1* [*time2*] [*time3*]
10. **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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the HTTP server on the Cisco Unified CME router that hosts the service URL for the Extension Mobility Login and Logout pages.
Step 4	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

Step 5	**url authentication** *url-address application-name password*
	
	Example:
	`Router(config-telephony)# url authentication http://192.0.2.0/CCMCIP/authenticate.asp secretname psswrd`
	or
	To support Extension Mobility *and* VoiceView Express 3.2 or earlier versions
	`Router(config-telephony)# url authentication http://192.0.2.0/voiceview/authentication/authenticate.do secretname psswrd`
		Instructs phones to send HTTP requests to the authentication server and specifies which credential to use in the requests.
		• This command is supported in Cisco Unified CME 4.3 and later versions. Required to support Automatic Clear Call history.
		• URL for internal authentication server in Cisco Unified CME is **http://***CME IP Address***/CCMCIP/authenticate.asp**.

	Command or Action	Purpose
		• To support Extension Mobility and Cisco VoiceView Express 3.2 or an earlier version only: ◦ In Cisco Unified CME: Configure the **url authentication** command using the URL for Cisco Unity Express. The URL for Cisco Unity Express is **http://***CUE IP Address***/voiceview/authentication/authenticate.do**. ◦ In Cisco Unity Express: Configure the **fallback-url** command using the URL for the authentication server in Cisco Unified CME. ◦ See Examples, on page 733.
Step 6	**service phone webAccess 0** **Example:** `Router(config-telephony)# service phone webAccess 0`	Enables webAccess for IP phones. This is required for 9.x firmware because the web server is disabled by default. 8.x firmware and lower had the web server enabled by default.
Step 7	**authentication credential** *application-name password* **Example:** `Router(config-telephony)#authentication credential secretname psswrd`	(Optional) Creates an entry for an application's credential in the database used by the Cisco Unified CME authentication server. • This command is supported in Cisco Unified CME 4.3 and later versions. • Required to support requests requests from applications other than Extension Mobility, such as Cisco VoiceView Express.
Step 8	**em keep-history** **Example:** `Router(config-telephony)# em keep-history`	(Optional) Specifies that Extension Mobility will keep, and not automatically clear, call histories when users log out from Extension Mobility phones. • This command is supported in Cisco Unified CME 4.3 and later versions. • Default: Automatic Clear Call History is enabled.
Step 9	**em logout** *time1* [*time2*] [*time3*] **Example:** `Router(config-telephony)# em logout 19:00 24:00`	(Optional) Defines up to three time-of-day timers for automatically logging out all Extension Mobility users. • This command is supported in Cisco Unified CME 4.3 and later versions. • *time*—Time of day after which logged-in users are automatically logged out from Extension Mobility. Range: 00:00 to 24:00 on a 24-hour clock.

	Command or Action	Purpose
		• To configure a idle-duration timer for automatically logging out an individual user, see Configure a User Profile, on page 741.
Step 10	**end** **Example:** `Router(config-telephony)# end`	Exits configuration mode and returns to privileged EXEC mode.

Examples

The following example shows how to configure Cisco Unified CME 4.3 or a later version and Cisco Unity Express 3.2 or an earlier version to support Extension Mobility and Cisco VoiceView Express.

Note: When running Extension Mobility and Cisco VoiceView Express 3.2 or an earlier version, you must also configure the **fallback-url** command in Cisco Unity Express. For configuration information, see the appropriate Cisco Unity Express Administrator Guide.

Cisco Unified CME 4.3 or a later version

```
telephony-service
 url authentication http://192.0.2.0/voiceview/authentication/authenticate.do secretname
psswrd
 authentication credentials secretname psswrd
```

Cisco Unity Express 3.2 or an earlier version

```
service phone-authentication
 fallback-url http://192.0.2.0/CCMCIP/authenticate.asp?UserID=secretname&Password=psswrd
```

Configure a Logout Profile for an IP Phone

To create a logout profile to define the default appearance for a Cisco Unified IP phone that is enabled for Extension Mobility, perform the following steps.

Restriction

- For button appearance, Extension Mobility associates directory numbers, then speed-dial definitions in the logout profile or user profile to phone buttons. The sequence in which directory numbers are associated is based on line type and ring behavior as follows: first normal, then silent ring, beep ring, feature ring, monitor ring, and overlay, followed by speed dials. If the profile contains more directory numbers and speed-dial numbers than there are buttons on the physical phone to which the profile is downloaded, not all numbers are downloaded to buttons.
- The first number to be configured for line appearance cannot be a monitored directory number.
- The user name parameter of any authentication credential must be unique. Do not use the same value for a user name when you configure any two or more authentication credentials in Cisco Unified CME, such as the user name for any Cisco Unified CME GUI account and the user name in a logout or user profile for Extension Mobility.

Before You Begin

- All directory numbers to be included in a logout profile or a user profile must be already configured in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.
- For Privacy on extension mobility phones, Cisco Unified 4.3 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice logout-profile** *profile-tag*
4. **user** *name* **password** *password*
5. **number** *number* **type** *type*
6. **speed-dial** *speed-tag number* [**label** *label*] [**blf**]
7. **pin** *number*
8. **privacy-button**
9. **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.

	Command or Action	Purpose
Step 3	**voice logout-profile** *profile-tag* **Example:** `Router(config)# voice logout-profile 1`	Enters voice logout-profile configuration mode for creating a logout profile to define the default appearance for a Cisco Unified IP phone enabled for Extension Mobility. • *profile-tag*—Unique number that identifies this profile during configuration tasks. Range: 1 to maximum number of phones supported by the Cisco Unified CME router. Type **?** to display the maximum number.
Step 4	**user** *name* **password** *password* **Example:** `Router(config-logout-profile)# user 23C2-8 password 43214`	Creates credential to be used by a TAPI phone device to log into Cisco Unified CME. • *name*—Unique alphanumeric string to identify a user for this authentication credential only. • *password*—Alphanumeric string.

Step 5	**number** *number* **type** *type*
	
	Example:
	`Router(config-logout-profile)# number 3001 type silent-ring`
	`Router(config-logout-profile)# number 3002 type beep-ring`
	`Router(config-logout-profile)# number 3003 type feature-ring`
	`Router(config-logout-profile)# number 3004 type monitor-ring`
	`Router(config-logout-profile)# number 3005,3006 type overlay`
	`Router(config-logout-profile)# number 3007,3008 type cw-overly`
		Creates line definition.
		• *number*—Directory number to be associated with and displayed next to a button on a Cisco Unified IP phone that is configured with this profile.
		• [**,** *...number*]—(Optional) For overlay lines only, with or without call waiting. The directory number that is the far left in command list is the highest priority. Can contain up to 25 numbers. Individual numbers must be separated by commas (**,**).
		• **type** *type*—Denotes characteristics to be associated with this line. Type **?** for list of options.

Step 6	**speed-dial** *speed-tag number* [**label** *label*] [**blf**]
	
	Example:
	`Router(config-logout-profile)# speed-dial 1 2001`
	`Router(config-logout-profile)# speed-dial 2 2002 blf`
		Creates speed-dial definition.
		• *speed-tag*—Unique sequence number that identifies a speed-dial definition during configuration tasks. Range: 1 to 36.
		• *number*—Digits to be dialed when the speed-dial button is pressed.
		• **label** *label*—(Optional) String that contains identifying text to be displayed next to the speed-dial button. Enclose the string in quotation marks if the string contains a space.
		• **blf**—(Optional) Enables Busy Lamp Field (BLF) monitoring for a speed-dial number.

Step 7	**pin** *number* **Example:** `Router(config-logout-profile)# pin 1234`	Sets a personal identification number (PIN) to be used by a phone user to disable the call blocking configuration for a Cisco Unified IP phone on which this profile is downloaded. • *number*—Numeric string containing four to eight digits.

	Command or Action	Purpose
Step 8	**privacy-button** **Example:** `Router(config-logout-profile)# privacy-button`	(Optional) Enables the privacy feature button on the IP phone. • Enable this command only on phones that share an octo-line directory number. • This command is supported in Cisco Unified CME 4.3 and later versions.
Step 9	**end** **Example:** `Router(config-logout-profile)# end`	Exits to privileged EXEC mode.

Enable an IP Phone for Extension Mobility

To enable the Extension Mobility feature on an individual Cisco Unified IP phone in Cisco Unified CME, perform the following steps.

Note All SCCP Cisco Unified IP phones with displays that support URL provisioning for Feature buttons are supported by Extension Mobility, including the Cisco Unified Wireless IP Phone 7920, Cisco Unified Wireless IP Phone 7921, and Cisco IP Communicator.

Restriction

- Extension Mobility is not supported on Cisco Unified IP phones without phone screens.
- Extension Mobility is not supported for analog devices.

Before You Begin

- HTTP server is enabled on the Cisco Unified CME router. For configuration information, see Configure Cisco Unified CME for Extension Mobility, on page 730.
- Logout profile to be assigned to a phone must be configured in Cisco Unified CME.
- Cisco IP Communicator to be enabled for Extension Mobility must be already registered in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mac-address** *mac-address*
5. **type** *phone-type*
6. **logout-profile** *profile-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	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enables phone configuration mode. • *phone-tag*—Unique number that identifies this phone during configuration tasks. Range is 1 to maximum number supported phones, where maximum is platform and version dependent and defined by using the **max-ephone** command.
Step 4	**mac-address** *mac-address* **Example:** `Router(config-ephone)# mac-address 000D.EDAB.3566`	Associates a physical phone with this ephone configuration.
Step 5	**type** *phone-type* **Example:** `Router(config-ephone)# type 7960`	Defines a phone type for the phone being configured.
Step 6	**logout-profile** *profile-tag* **Example:** `Router(config-ephone)# logout-profile 1`	Enables Cisco Unified IP phone for Extension Mobility and assigns a logout profile to this phone. • *tag*—Unique identifier of logout profile to be used when no phone user is logged in to this phone. This tag number corresponds to a tag number created when this logout profile was configured by using the **voice logout-profile** command.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Configure Extension Mobility for SIP Phones

To prepare Extension Mobility for use with SIP phones, perform the following steps.

Before You Begin

- Cisco IOS Release 15.1(4)M.
- Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **voice register global**
5. **url authentication** *url-address application-name password*
6. **exit**
7. **telephony-service**
8. **authentication credential** *application-name password*
9. **em keep-history**
10. **em logout** *time1* [*time2*] [*time3*]
11. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip http server** **Example:** `Router(config)# ip http server`	Enables the HTTP server on the Cisco Unified CME router which hosts the service URL for the Extension Mobility login and logout pages.
Step 4	**voice register global** **Example:** `Router(config)# voice register global`	Defines global voice register commands.
Step 5	**url authentication** *url-address application-name password* **Example:** `Router(config-register-global)# url authentication http://192.0.2.0/CCMCIP/authenticate.asp secretname psswrd`	Instructs phones to send HTTP requests to the authentication server and specifies which credential to use in the requests. • Required to support Automatic Clear Call history. • application-name—user name you choose and define in this command. • password—password you define using this command. • URL—URL address for the authentication server in Cisco Unified CME is **http://***CMEIP Address***/CCMCIP/authenticate.asp**.
Step 6	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global confiuration mode.
Step 7	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony service configuration mode.
Step 8	**authentication credential** *application-name password* **Example:** `Router(config-telephony)# authentication credential` **application-name password**	Specifies authorized credentials. Use credentials from Step 5. **Note** This step is needed only when you set the CME internal authentication server as your phone authentication server in Step 5.
Step 9	**em keep-history** **Example:** `Router(config-telephony)# em keep-history`	(Optional) Specifies that Extension Mobility will keep, and not automatically clear, call histories when users log out from Extension Mobility phones. **Note** Default: Automatic Clear Call History is enabled.

	Command or Action	Purpose
Step 10	**em logout** *time1* [*time2*] [*time3*] **Example:** `Router(config-telephony)# em logout 19:00 24:00`	(Optional) Defines up to three time-of-day timers for automatically logging out all Extension Mobility users. • *time*—Time of day after which logged-in users are automatically logged out from Extension Mobility. Range: 00:00 to 24:00 on a 24-hour clock.
Step 11	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Enable SIP Phones for Extension Mobility

To enable the Extension Mobility feature on a SIP phone in Cisco Unified CME, perform the following steps.

> **Note** All Cisco Unified SIP phones with displays that support URL provisioning are supported by Extension Mobility.

Before You Begin

- HTTP server is enabled on the Cisco Unified CME router.
- Default logout and user profiles to be assigned to a phone must be configured in Cisco Unified CME.
- The voice register directory numbers in default logout and user profiles must be configured in Cisco Unified CME. To configure SIP directory numbers, see Cisco Unified Communications Manager Express Command Reference Guide.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **id mac** *mac-address*
5. **type** *phone-type*
6. **logout-profile** *profile-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	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 22`	Enables phone configuration mode. • pool-tag—Unique number that identifies this register pool during configuration tasks. Range is 1 to 42.
Step 4	**id mac** *mac-address* **Example:** `Router(config-register-pool)# id mac 0123.4567.89AB`	Associates a physical phone with this ephone configuration. • mac-address—mac address of the physical phone
Step 5	**type** *phone-type* **Example:** `Router(config-register-pool)# type 7970`	Defines a phone type for the phone being configured.
Step 6	**logout-profile** *profile-tag* **Example:** `Router(config-register-pool)# logout-profile 22`	Enables Cisco Unified SIP phone for Extension Mobility and assigns a logout profile to this phone. • profile tag—Unique identifier of a logout profile to be used when no phone user is logged in to this phone. This tag number corresponds to a tag number created when this logout profile was configured by using the **voice logout-profile** command.
Step 7	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Configure a User Profile

To configure a user profile for a phone user who logs into a Cisco Unified IP phone that is enabled for Extension Mobility, perform the following steps.

Note Templates created using the **ephone-template** and **ephone-dn-template** commands can be applied to a user profile for Extension Mobility.

Restriction

- For button appearance, Extension Mobility associates directory numbers, then speed-dial definitions in the logout profile or user profile to phone buttons. The sequence in which directory numbers are associated is based on line type and ring behavior as follows: first normal, then silent ring, beep ring, feature ring, monitor ring, and overlay, followed by speed dials. If the profile contains more directory numbers and speed-dial numbers than there are buttons on the physical phone to which the profile is downloaded, not all numbers are downloaded to buttons.
- The first number to be configured for line appearance cannot be a monitored directory number.
- The user name parameter of any authentication credential must be unique. Do not use the same value for a user name when you configure any two or more authentication credentials in Cisco Unified CME, such as the user name for any Cisco Unified CME GUI account and the user name in a logout or user profile for Extension Mobility.

Before You Begin

- All directory numbers to be included in a logout profile or user profile must be already configured in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.
- For Automatic Logout, Cisco Unified CME 4.3 or a later version.
- For Privacy on extension mobility phones, Cisco Unified CME 4.3 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice user-profile** *profile-tag*
4. **user** *name* **password** *password*
5. **number** *number* **type** *type*
6. **speed-dial** *speed-tag number* [**label** *label*] [**blf**]
7. **pin** *number*
8. **max-idle-time** minutes
9. **privacy-button**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice user-profile** *profile-tag* **Example:** `Router(config)# voice user-profile 1`	Enters voice user-profile configuration mode for configuring a user profile for Extension Mobility. • *profile-tag*—Unique number that identifies this profile during configuration tasks. Range: 1 to three times the maximum number supported phones, where maximum is platform dependent. Type **?** to display value.
Step 4	**user** *name* **password** *password* **Example:** `Router(config-user-profile)# user me password pass123`	Creates credential to be authenticated by Cisco Unified CME before allowing the phone user to log into a Cisco Unified IP phone phone enabled for Extension Mobility. • *name*—Unique alphanumeric string to identify a user for this authentication credential only. • *password*—Password for authorized user.

Step 5	**number** *number* **type** *type*
	
	Example:
	`Router(config-user-profile)# number 2001 type silent-ring`
	`Router(config-user-profile)# number 2002 type beep-ring`
	`Router(config-user-profile)# number 2003 type feature-ring`
	`Router(config-user-profile)# number 2004 type monitor-ring`
	`Router(config-user-profile)# number 2005,2006 type overlay`
	`Router(config-user-profile)# number 2007,2008 type cw-overly`
		Creates line definition.
		• *number*—Directory number to be associated with and displayed next to a button on a phone that is configured with this profile.
		• [**,** *...number*]—(Optional) For overlay lines only, with or without call waiting. The directory number that is far left in the command list is given the highest priority. Can contain up to 25 numbers. Individual numbers must be separated by commas (**,**)
		• **type** *type*—Denotes characteristics to be associated with this line. Type ? for list of options.

Step 6	**speed-dial** *speed-tag number* [**label** *label*] [**blf**]
	
	Example:
	`Router(config-user-profile)# speed-dial 1 3001`
	
	`Router(config-user-profile)# speed-dial 2 3002 blf`
		Creates speed-dial definition.
		• *speed-tag*—Unique sequence number that identifies a speed-dial definition during configuration tasks. Range: 1 to 36.
		• *number*—Digits to be dialed when the speed-dial button is pressed.
		• **label** *label*—(Optional) String that contains identifying text to be displayed next to the speed-dial button. Enclose the string in quotation marks if the string contains a space.

	Command or Action	Purpose
		• **blf**—(Optional) Enables Busy Lamp Field (BLF) monitoring for a speed-dial number.
Step 7	**pin** *number* **Example:** `Router(config-user-profile)# pin 12341`	Sets a personal identification number (PIN) to be used by a phone user to disable the call blocking configuration for a Cisco Unified IP phone on which this profile is downloaded. • *number*—Numeric string containing four to eight digits.
Step 8	**max-idle-time** minutes **Example:** `Router(config-user-profile)# max-idle-time 30`	(Optional) Creates an idle-duration timer for automatically logging out an Extension Mobility user. • This command is supported in Cisco Unified CME 4.3 and later versions. • *minutes*—Maximum number of minutes after which a user is logged out from an idle Extension Mobility phone. Range:1 to 9999.
Step 9	**privacy-button** **Example:** `Router(config-user-profile)# privacy-button`	(Optional) Enables the privacy feature button on the IP phone. • Enable this command only on phones that share an octo-line directory number. • This command is supported in Cisco Unified CME 4.3 and later versions.
Step 10	**end** **Example:** `Router(config-user-profile)# end`	Exits to privileged EXEC mode.

Configuration Examples for Extension Mobility

Example for Configuring Extension Mobility for Use with SIP Phones

The following example shows a sample configuration for enabling Extension Mobility for use with SIP phones:

```
Router#en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#ip http server
Router(config)#voice register global
Router(config-register-global)#$.2.0/CCMCIP/authenticate.asp admin password
Router(config-register-global)#exit
Router(config)#telephony-service
Router(config-telephony)#authentication credential admin password
```

```
Router(config-telephony)#em keep-history
Router(config-telephony)#em logout 19:00
Router(config-telephony)#end
```

Example for Configuring SIP Phones for Use with Extension Mobility

The following example shows a sample configuration for enabling a SIP phone to use Extension Mobility:

```
Router#en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router#en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#voice register pool 1
Router(config-register-pool)#id mac 12.34.56
Router(config-register-pool)#type 7960
Router(config-register-pool)#logout-profile 22
Enabling extension mobility will replace current phone configuration with logout
 profile, continue?? [yes]: y
Router(config-register-pool)#end
```

Example for Configuring Logout Profile

The following example shows the configuration for a logout profile that defines the default appearance for a Cisco Unified IP phone that is enabled for Extension Mobility. Which lines and speed-dial buttons in this profile are configured on a phone depends on the phone type. For example, for a Cisco Unified IP Phone 7970, all buttons are configured according to logout profile1. However, if the phone is a Cisco Unified IP Phone 7960, all six lines are mapped to phone buttons and the speed dial is ignored because there is no button available for speed dial.

```
voice logout-profile 1
 pin 9999
 user 23C2-8 password 43214
 number 3001 type silent-ring
 number 3002 type beep-ring
 number 3003 type feature-ring
 number 3004 type monitor-ring
 number 3005,3006 type overlay
 number 3007,3008 type cw-overly
 speed-dial 1 2000
 speed-dial 2 2001 blf
```

Example for Enabling an IP Phone for Extension Mobility

The following example shows the ephone configurations for three IP phones. All three phones are enabled for Extension Mobility and share the same logout profile number 1, to be downloaded when these phones boot and when no phone user is logged into the phone.

```
ephone 1
 mac-address 000D.EDAB.3566
 type 7960
 logout-profile 1

ephone 2
 mac-address 0012.DA8A.C43D
 type 7970
 logout-profile 1
```

```
ephone 3
 mac-address 1200.80FC.9B01
 type 7911
 logout-profile 1
```

Example for Configuring User Profile

The following example shows the configuration for a user profile to be downloaded when a phone user logs into a Cisco Unified IP phone that is enabled for Extension Mobility. Which lines and speed-dial buttons in this profile are configured on a phone after the user logs in depends on the phone type. For example, if the user logs into a Cisco Unified IP Phone 7970, all buttons are configured according to voice-user profile1. However, if the phone user logs into a Cisco Unified IP Phone 7960, all six lines are mapped to phone buttons and the speed dial is ignored because there is no button available for speed dial.

```
voice user-profile 1
 pin 12345
 user me password pass123
 number 2001 type silent-ring
 number 2002 type beep-ring
 number 2003 type feature-ring
 number 2004 type monitor-ring
 number 2005,2006 type overlay
 number 2007,2008 type cw-overly
 speed-dial 1 3001
 speed-dial 2 3002 blf
```

Where to Go Next

- If you created a new or modified an existing logout or user profile, you must restart the phones to propagate the changes. See Reset and Restart Cisco Unified IP Phones, on page 397.
- If you enabled one or more Cisco Unified IP phones for Extension Mobility, generate a new configuration file and restart the phones. See Configuration Files for Phones, on page 387.

Feature Information for Extension Mobility

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

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

Table 51: Feature Information for Extension Mobility

Feature Name	Cisco Unified CME Version	Modification
MIB Support for Extension Mobility in Cisco Unified SCCP IP Phones	9.0	Adds new MIB objects to monitor Cisco Unified SCCP IP EM phones.
Support for SIP phones	8.6	Adds support for SIP phones.

Feature Name	Cisco Unified CME Version	Modification
Extension Mobility Enhancement	7.0/4.3	Adds support for the following: • Automatic Logout, including: • Configurable time-of-day timers for automatically logging out all Extension Mobility users. • Configurable idle-duration timer for logging out an individual user from an idle Extension Mobility phone. • Automatic Clear Call History when a user logs out from Extension Mobility.
Phone User-Interface for Speed Dial	7.0/4.3	Adds a phone user interface allowing Extension Mobility users to configure their own speed-dial settings directly on the phone.
Extension Mobility	4.2	Provides the benefit of phone mobility for end users by enabling the user to log into any local Cisco Unified IP Phone that is enabled for Extension Mobility.

CHAPTER 22

Fax Relay

This chapter describes how to enable Skinny Client Control Protocol (SCCP) Fax Relay for analog foreign exchange service (FXS) ports under the control of Cisco Unified CME.

Prerequisites for Fax Relay

- Cisco Unified CME 4.0(3) or a later version.
- If your voice gateway is a separate router than the Cisco Unified CME router, an IP voice image of Cisco IOS Release 12.4(11)T or later is required.
- SCCP Telephony Control (STC) application is enabled.

Note

- For Cisco Unified CME versions before Cisco Unified CME 4.0(3), there are two manually-controlled options for setting up facsimiles:
    - Fax Gateway Protocol

      Configure the Cisco VG224, FXS port, or analog telephone adaptor (ATA) to use H.323 or Session Initiation Protocol (SIP) with a specific fax relay protocol. See Fax, Modem, and Text Support over IP Configuration Guide.

    - G.711 Fax Pass-Through with SCCP

      This is the default setup for facsimile on the Cisco VG224 and FXS ports before Cisco Unified CME 4.0(3). See Fax, Modem, and Text Support over IP Configuration Guide.

Restrictions for Fax Relay

- RFC2833 dual tone multifrequency (DTMF) digit relay under Cisco Unified CME for SCCP FXS ports is not supported.
- SCCP FXS ports under Cisco Unified CME control do not natively support RFC2833 DTMF-relay. However, Cisco Unified CME can support conversion of DTMF digits to and from RFC2833 DTMF-relay on its H323 and SIP interfaces when used with SCCP-controlled FXS ports.
- Cisco Fax Relay is only supported on those Cisco IOS gateways and network modules listed in Table 52: Supported Gateways, Modules, and VICs for Fax Relay , on page 752.

Information About Fax Relay

Fax Relay and Equipment

- The fax relay feature supports the use of existing customer premises equipment (CPE) in voice networks by allowing legacy analog phones attached to a Cisco IOS gateway to be controlled by Cisco Unified CME, and by providing feature interoperability between analog and IP endpoints.
- The voice gateway can be the same router that is being used for Cisco Unified CME or it may be a separate router (for example, the Cisco VG224).
- The fax relay feature facilitates replacement of the PSTN time-division multiplexing (TDM) infrastructure with VoIP.

Feature Design of Cisco Fax Relay

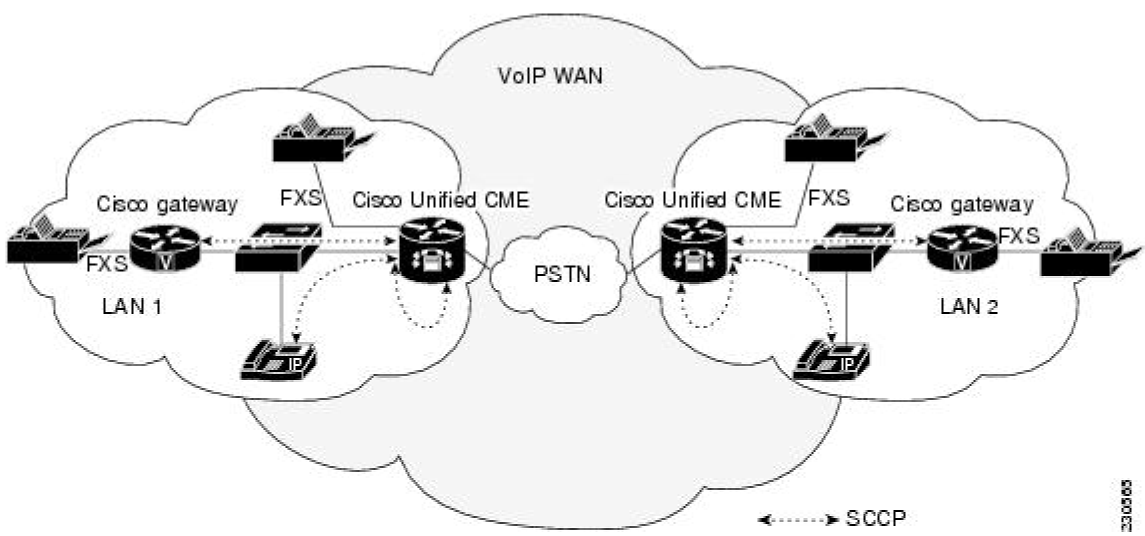
Cisco Fax Relay is a proprietary fax relay implementation that uses Real-time Transport Protocol (RTP) to transport fax data. It is the default fax relay type on Cisco voice gateways and the only supported fax option for Cisco Unified CME 4.0(3) and later versions. The fax relay feature provides enhanced supplementary feature capability on analog ports connected to a Cisco integrated services router (ISR) or Cisco VG224 analog gateway. Calls through the analog FXS ports are controlled by the Cisco Unified CME system.

Before the introduction of SCCP-enhanced features, SCCP gateways supported fax pass-through only. SCCP-enhanced features add support for Cisco Fax Relay and Super Group 3 (SG3) to G3 fax relay. This feature allows the fax stream between two SG3 fax machines to negotiate down to G3 speeds (less than 14.4 kbps) allowing SG3 fax machines to interoperate over fax relay with G3 fax machines.

The SCCP telephony control (STC) application on the Cisco voice gateway presents the locally attached analog telephones as individual endpoints to the call-control system, which allows the analog phones to be controlled in the same way as IP phones. With this capability, gateway-attached endpoints share the same telephony features that are available on IP phones directly connected to Cisco Unified CME. SCCP-enhanced features provide analog endpoint to analog endpoint interoperability within the IP telephony network.

Figure 26: Cisco Unified CME Fax Relay Deployment, on page 751 shows a multisite deployment of the fax relay feature in a Cisco Unified CME topology.

Figure 26: Cisco Unified CME Fax Relay Deployment



For information on configuring gateway-controlled fax relay features, see Configure Fax Relay, on page 753.

Supported Gateways, Modules, and Voice Interface Cards for Fax Relay

Table 52: Supported Gateways, Modules, and VICs for Fax Relay , on page 752 lists supported gateways, modules, and voice interface cards (VICs).

Table 52: Supported Gateways, Modules, and VICs for Fax Relay

Gateways	Extension Modules	Network Modules and Expansion Modules	VICs
• Cisco 2801 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845	—	• NM-HD-1V • NM-HD-2V • NM-HD-2VE	• VIC2-2FXS • VIC-4FXS/DID • VIC2-2BRI-NT/TE
• Cisco 2801 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845	• EVM-HD	• EVM-HD-8FXS/DID • EM-3FXS/4FXO • EM-HDA-8FXS • EM-4BRI-NT/TE	—
• Cisco 2801 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3825 • Cisco 3845	—	• NM-HDV2 • NM-HDV2-1T1/E1 • NM-HDV2-2T1/E1	• VIC2-2FXS • VIC-4FXS/DID • VIC2-2BRI-NT/TE
• Cisco VG 224	—	—	—

Configure Fax Relay

Configure Fax Relay on SCCP Phones

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **fax protocol cisco**
5. **fax-relay sg3-to-g3**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode and specifies VoIP encapsulation.
Step 4	**fax protocol cisco** **Example:** `Router(config-voi-serv)# fax protocol cisco`	Specifies the Cisco-proprietary fax protocol as the fax protocol for SCCP analog endpoints. • This command is enabled by default. • This is the only supported option for Cisco Unified CME 4.0(3) and later versions.
Step 5	**fax-relay sg3-to-g3** **Example:** `Router(config-voi-serv)# fax relay sg3-to-g3`	(Optional) Enables the fax stream between two SG3 fax machines to negotiate down to G3 speeds.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits the current configuration mode.

Verify and Troubleshoot Fax Relay Configuration

To verify the Cisco Fax Relay configuration, use the **show-running config** command. Sample output is located in the Example for Configuring Fax Relay, on page 754.

Use the following commands to verify and troubleshoot SCCP gateway-controlled Fax Relay:

- **show voice call summary—**Displays fax relay voice port settings.
- **show voice dsp—**Displays fax relay digital signal processor (DSP) channel status.
- **debug voip application stcapp all—** Displays SCCP telephony control (STC) application fax relay information.
- **debug voip dsm all—**Displays fax relay DSP stream manager (DSM) messages.
- **debug voip dsmp all—**Displays fax relay distributed stream media processor (DSMP) messages.
- **debug voip hpi all—**Displays gateway DSP fax relay information on RTP packet events.
- **debug voip vtsp all—**Displays gateway voice telephony service provider (VTSP) debugging information for fax calls.

Note For more information on these and other commands, see Cisco IOS Voice Command Reference, Cisco Unified Communications Manager Express Command Reference, and Cisco IOS Configuration Fundamentals Command Reference.

Configuration Examples for Fax Relay

Example for Configuring Fax Relay

```
voice service voip
   fax-relay sg3-to-g3

  ephone-dn 44
   number 1234
   name fax machine

  ephone 33
   mac-address 1111.2222.3333
```

```
button 1:44
type anl
```

Feature Information for Fax Relay

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

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

Table 53: Feature Information for Cisco Fax Relay

Feature Name	Cisco Unified CME Version	Feature Information
Fax Relay	4.0(3)	Enables Fax Relay on analog FXS ports on Cisco IOS voice gateways under the control of Cisco Unified CME.

CHAPTER 23

Feature Access Codes

Information About Feature Access Codes

Feature Access Codes

Feature Access Codes (FACs) are special patterns of characters that are dialed from a telephone keypad to invoke particular features. For example, a phone user might press **1, then press 2345 to forward all incoming calls to extension 2345.

Typically, FACs are invoked using a short sequences of digits that are dialed using the keypad on an analog phone, while IP phone users select softkeys to invoke the same features. In Cisco Unified CME 4.0 and later, the same FACs that are available for analog phones can be enabled on IP phones. This allows phone users to select a particular feature or activate/deactivate a function in the same manner regardless of phone type.

FACs are disabled on IP phones until they are explicitly enabled. You can enable all standard FACs for all SCCP phones registered in Cisco Unified CME or you can define a custom FAC or alias to enable one or more individual FACs.

All FACs except the call-park FAC are valid only immediately after a phone is taken off hook. The call-park FAC is considered a transfer to a call-park slot and therefore is only valid after the Transfer softkey (IP phones) or hookflash (analog phones) is used to initiate a transfer.

Note Directory Numbers configured on the Unified CME router should not overlap with the numbers you assign for FAC Standard or FAC Custom in a FAC configuration. Also, ensure that the FAC code always starts with an asterisk, followed by digits.

Table 54: Standard Feature Access Codes, on page 758 contains a list of the standard predefined FACs.

Table 54: Standard Feature Access Codes

Standard FAC	Description
**1 plus optional extension number	Call forward all.
**2	Call forward all cancel.
**3	Pick up local group.
**4 plus group number	Pick up a ringing call in the specified pickup group. Specified pickup group must already configured in Cisco Unified CME.
**5 plus extension number	Pick up direct extension.
**6 plus optional park-slot number	Call park, if the phone user has an active call and if the phone user presses the Transfer softkey (IP phone) or hookflash (analog phone) before dialing this FAC. Target park slot must be already configured in Cisco Unified CME.
**7	Do not disturb.
**8	Redial.
**9	Dial voice-mail number.
*3 plus hunt group pilot number	Join ephone-hunt group. If multiple hunt groups have been created that allow dynamic membership, the hunt group to be joined is identified by its pilot number.
*4	Activate or deactivate hunt group logout functionality to toggle between ready/not-ready status of an extension when the hunt group agent is off-hook.
*5	Activate or deactivate phone-level hunt group logout to toggle between ready/not-ready status of all extensions on a individual phone that is a member of an ephone hunt group when the phone is idle.
*6	Dials the voice-mail number.
#3	Leave ephone-hunt group. Telephone or extension number must already be configured as a dynamic member of a hunt group.

Configure Feature Access Codes

To enable standard FACs or create custom FACs, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **fac** {**standard** | **custom** {**alias** *alias-tag custom-fac* **to** *existing-fac* [*extra-digits*]} | *feature custom-fac*}}
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**fac** {**standard** | **custom** {**alias** *alias-tag custom-fac* **to** *existing-fac* [*extra-digits*]} | *feature custom-fac*}} **Example:** `Router(config-telephony)# fac custom callfwd *#5`	Enables standard FACs or creates a custom FAC or alias. • **standard—**Enables standard FACs for all phones. • **custom—**Creates a custom FAC for a FAC type. • **alias—**Creates a custom FAC for an existing FAC or a existing FAC plus extra digits. • *alias-tag*—Unique identifying number for this alias. Range: 0 to 9. • *custom-fac*—User-defined code to be dialed using the keypad on an IP or analog phone. Custom FAC can be up to 256 characters long and contain numbers 0 to 9 and * and #. • **to—**Maps custom FAC to specified target. • *existing-fac*—Already configured custom FAC that is automatically dialed when the phone user dials the custom FAC being configured.

	Command or Action	Purpose
		• *extra-digits*—(Optional) Additional digits that are automatically dialed when the phone user dials the custom FAC being configured. • *feature*—Predefined alphabetic string that identifies a particular feature or function. Type **?** for a list.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify Feature Access Codes

To verify the FAC configuration, perform the following step.

show telephony-service fac

Example:
This command displays a list of FACs that are configured on the Cisco Unified CME router. The following example shows the output when standard FACs are enabled:

```
Router# show telephony-service fac

telephony-service fac standard
 callfwd all **1
 callfwd cancel **2
 pickup local **3
 pickup group **4
 pickup direct **5
 park **6
 dnd **7
 redial **8
 voicemail **9
 ephone-hunt join *3
 ephone-hunt cancel #3
 ephone-hunt hlog *4
 ephone-hunt hlog-phone *5
 trnsfvm *6
```

The following example shows the output when custom FACs are configured:

```
Router# show telephony-service fac

telephony-service fac custom
 callfwd all #45
 alias 0 #1 to **4121
 alias 1 #2 to **4122
 alias 4 #4 to **4124
```

Configuration Examples for Feature Access Codes

Example for Enabling Standard FACs for All Phones

The following example shows how to enable standard FACs for all phones:

```
Router# telephony-service
Router(config-telephony)# fac standard
fac standard is set!
Router(config-telephony)#
```

The following example shows how the standard FAC for the Call Forward All feature is changed to a custom FAC (#45). Then an alias is created to map a second custom fac to #45 plus an extension (1111). The custom FAC (#44) allows the phone user to press #44 to forward all calls to extension 1111, without requiring the phone user to dial the extra digits that are the extension number.

```
Router# telephony-service
Router(config-telephony)# fac custom callfwd all #45
fac callfwd all code has been configured to #45
Router(config-telephony)# fac custom alias 0 #44 to #451111
fac alias0 code has been configurated to #44!
alias0 map code has been configurated to #451111!
```

The following example shows how to define an alias for the group pickup of group 123. The alias substitutes the digits #4 for the standard FAC for group pickup (**4) and adds the group number (123) to the dial pattern. Using this custom FAC, a phone user can dial #4 to pick up a ringing call in group 123, instead of dialing the standard FAC **4 plus the group number 123.

```
Router# telephony-service
Router(config-telephony)# fac custom alias 5 #4 to **4123
```

Feature Information for Feature Access Codes

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

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

Table 55: Feature Information for Feature Access Codes

Feature Name	Cisco Unified CME Version	Feature Information
Transfer to Voice Mail.	7.0/4.3	FAC for Transfer to Voice Mail was added.

Feature Name	Cisco Unified CME Version	Feature Information
Feature Access Codes (FACs)	4.0	FACs were introduced.

CHAPTER 24

Forced Authorization Code

Information About Forced Authorization Code

Forced Authorization Code Overview

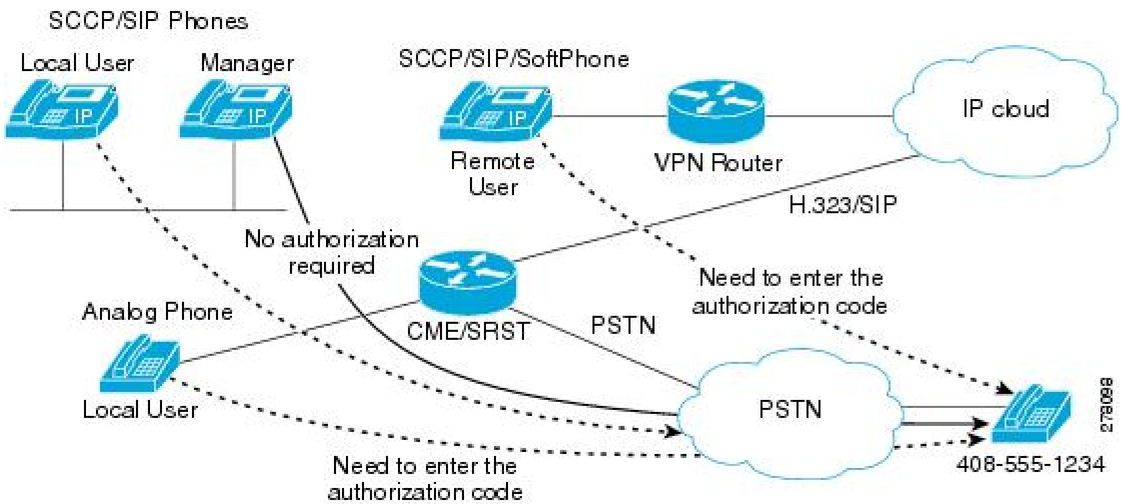
Cisco Unified CME 8.5 allows you to manage call access and call accounting through the Forced Authorization Code (FAC) feature. The FAC feature regulates the type of call a certain caller may place and forces the caller to enter a valid authorization code on the phone before the call is placed. FAC allows you to track callers dialing non-toll-free numbers, long distance numbers, and also for accounting and billing purposes.

In Cisco Unified CME and Cisco Voice Gateways, devices and endpoints are logically partitioned into different logical partitioning class of restriction (LPCOR) groups. For example, IP phones, Analog phones, PSTN trunks, and IP (h323/SIP) trunks as shown in Figure 27: Forced Authorization Code Network Overview, on page 764, are partitioned into five LPCOR groups under the voice lpcor custom mode, such as:

- voice lpcor custom
- group 10 Manager
- group 11 LocalUser
- group 12 RemoteUser
- group 13 PSTNTrunk

- group 14 IPTrunk

Figure 27: Forced Authorization Code Network Overview



For each group, the LPCOR group policy of a routing endpoint is enhanced to define incoming calls from individual LPCOR groups that are restricted by FAC. A LPCOR group call to a destination is accepted only when a valid FAC is entered. FAC service for a routing endpoint is enabled through the service fac defined in a LPCOR group policy. For more information, see Enable Forced Authorization Code (FAC) on LPCOR Groups, on page 770.

The following are the group policy rules applicable to the PSTNTrunk LPCOR group:

- FAC is required by PSTNTrunk if a call is initiated from either LocalUser or RemoteUser group.
- Any calls from Manager group are allowed to terminate to PSTNTrunk without restriction.
- Any incoming calls from either IPTrunk or PSTNTrunk group are rejected and terminated to PSTNTrunk group.

For information on configuring LPCOR groups and associating LPCOR group with different device types, see Call Restriction Regulations, on page 1101.

FAC Call Flow

FAC is required for an incoming call based on the LPCOR policy defined for the call destination. Once the authentication is finished, the success or failure status and the collected FAC digits are saved to the call detail records (CDRs).

Calls are handled by a new built-in application authorization package which first plays a user-prompt for the caller to enter a username (in digits), then the application plays a passwd-prompt for the caller to collect the password (in digits). The collected username and password digits are then used for FAC, see Define Parameters for Authorization Package, on page 772.

When FAC authentication is successful, the outgoing call setup is continued to the same destination. If FAC authentication fails, the call is then forwarded to the next destination. FAC operations are invoked to the call if FAC service is enabled in the next destination and no valid FAC status is saved for the call.

Any calls failing because of FAC blocking are disconnected with a LPCOR Q.850 disconnect cause code. Once the FAC is invoked for a call, the collected authorization digits and the authentication status information is collected by call active or call history records. You can retrieve the FAC information through the **show call active voice** and **show call history voice** commands.

Forced Authorization Code Specification

The authorization code used for call authentication must follow these specifications:

- The authorization code must be in numeric (0 – 9) format.
- A digit collection operation must be completed if either one of the following conditions occur:
    - maximum number of digits are collected
    - digit input times out
    - a terminating digit is entered

Once digit collection is completed, the authentication is done by either the external Radius server or Cisco Unified CME or Cisco Voice Gateways by using AAA Login Authentication setup. For more information on AAA login authentication methods, see Configuring Authentication.

When authentication is done by local Cisco Unified CME or Cisco Voice Gateways, the **username** *ac-code* **password 0** *password* command is required to authenticate the collected authorization code digits.

FAC data is stored through the CDR and new **AAA fac-digits** and **fac-status** attributes and are supported in a CDR STOP record. This CDR STOP record is formatted for file accounting, RADIUS or Syslog accounting purpose.

FAC Requirement for Different Types of Calls

Table 56: FAC Support for Different Types of Calls, on page 765 shows FAC support for different types of calls.

Table 56: FAC Support for Different Types of Calls

Types of Calls	FAC Behavior for Different Calls
Basic Call	A calls B. B requires A to enter a FAC. A is routed to B only when A enters a valid FAC.
Call Forward All Call Forward Busy	When A (with no FAC) calls B, A is call forwarded to C: • No FAC is required when B enables Call Forward All or Call Forward Busy to C. • FAC is required on A when A is call forwarded to C.

Types of Calls	FAC Behavior for Different Calls
Call Forward No Answer	When A (with no FAC) calls B and A (with FAC) calls C: A calls B: • No FAC is required when A calls B. A is Call Forward No Answer (CFNA) to C. • FAC is required on A when A is call forward to C.
Call Transfer (Blind)	FAC is required, if B calls C and A, and A calls C. **Example:** A calls B. B answers the call. B initiates a blind transfer call to C. A is prompted to enter FAC. A is routed to C only if a valid FAC is entered by A.

<table>
<tr><th>Types of Calls</th><th>FAC Behavior for Different Calls</th></tr>
<tr><td>Call Transfer (Consultation)

Transfer Complete at Alerting State</td><td>
1 FAC is required if B calls C. FAC is not required when A calls C,

Example:

a A calls B. B answers the call and initiates a consultation transfer to C.

b B is prompted to enter a FAC and B is not allowed to complete the call transfer when FAC is not completed.

c B (the transfer call) is forwarded to C after a valid FAC is entered. B completes the transfer while the transfer call is still ringing on C. A is then transferred to C.

2 FAC is required if B calls C and A calls C.

Example:

a A calls B. B answers the call and initiates a consultation transfer to C.

b B is prompted to enter a FAC and B is not allowed to complete the call transfer when FAC is not completed.

c No FAC is required to A, A is then transferred to C.

3 FAC is not required if B calls C but FAC is required if A calls C.

Example:

a A calls B, B answers the call.

b B initiates a consultation transfer to C and completes the transfer.

c No FAC required to A, A is then transferred to C.
</td></tr>
</table>

Types of Calls	FAC Behavior for Different Calls
Transfer Complete at Connected State	1 FAC is required when A calls C. **Example:** **a** A calls B, B answers the call and initiates a consultation transfer to C. **b** C answers the transfer call and B completes the transfer. **c** No FAC required to connect to A (including local hairpin calls because the call transfer is complete) and A is connected to C.
Conference Call (Software/Adhoc)	1 FAC is not invoked when a call is joined to a conference connection. 2 FAC is required between A and C, B and C. **Example:** **a** A calls B, B answers the call and initiates a conference call to C. **b** B enters a valid authorization code and is routed to C. **c** C answers the conference call and the conference is complete. **d** No FAC is required to connect to A and A is joined to a conference connection.
Meetme Conference	1 FAC is not invoked for a caller to join the meetme conference. 2 FAC is required between A and C, B and C. **Example:** **a** C joins the meetme conference first. **b** No FAC is required if B joins the same meetme conference. **c** No FAC is required if C also joins the same meetme conference.

Types of Calls	FAC Behavior for Different Calls
Call Park and Retrieval	**1** FAC is not invoked for the parked call. **2** FAC is required if C calls A. **Example:** **a** A calls B, B answers the call and parks the caller on A. **b** C retrieves the parked call (A), no FAC is required to reach C, and C is connected to A.
Call Park Restore	**1** FAC is required if A calls D. **Example:** **a** A calls B, B answers the call and parks the caller on A. **b** Parked call (A) is timed out from a call-park slot and is forwarded to D. **c** No FAC is required for D and the parked call (A) will ring on D.
Group Pickup	**1** FAC is not provided if a caller picks up a group call. **2** FAC is required if C calls A. **Example:** **a** A calls B, A is ringing on B, and C attempts to pickup call A. **b** No FAC is required for C and C is connected to A.
Single Number Redirection (SNR)	FAC is not supported for an SNR call.
Third Party Call Control (3pcc)	FAC is not supported for a three-party call control (3pcc) outgoing call.
Parallel Hunt Groups	FAC is not supported on parallel hunt groups.
Whisper intercom	FAC is not supported for whisper intercom calls.

Configure Forced Authorization Code

Enable Forced Authorization Code (FAC) on LPCOR Groups

Restriction Authenticated FAC data is saved to a call-log from which the authorization code is collected. When a call-forward or blind transfer call scenario triggers a new call due to the SIP notify feature, the same caller is required to enter the authorization code again for FAC authentication.

Warning A FAC pin code must be unique and not the same as an extension number. Cisco Unified CME, Cisco Unified SRST, and Cisco Voice Gateways will not validate whether a collected FAC pin code matches an extension number.

Before You Begin

- You must enable the voice lpcor enable command before configuring FAC.
- Trunks (IP and PSTN) must be associated with phones into different LPCOR groups. See Associate a LPCOR Policy with Analog Phone or PSTN Trunk Calls, on page 1114 for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice lpcor enable**
4. **voice lpcor custom**
5. **group** *number lpcor-group*
6. **exit**
7. **voice lpcor policy** *lpcor-group*
8. **accept** *lpcor-group* **fac**
9. **service** *fac*
10. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice lpcor enable** **Example:** `Router(config)# voice lpcor enable`	Enables LPCOR functionality on the Cisco Unified CME router.
Step 4	**voice lpcor custom** **Example:** `Router(config)# voice lpcor custom`	Defines the name and number of LPCOR resource groups on the Cisco Unified CME router.

Step 5	**group** *number lpcor-group*
	
	Example:
	`Router(cfg-lpcor-custom)#group 10 Manager`
	`Router(cfg-lpcor-custom)#group 11 LocalUser`
	`Router(cfg-lpcor-custom)#group 12 RemoteUser`
	`Router(cfg-lpcor-custom)#group 13 PSTNTrunk`
	`Router(cfg-lpcor-custom)#group 14 IPTrunk`
		Adds a LPCOR resource group to the custom resource list.
		• *number*—Group number of the LPCOR entry. Range: 1 to 64.
		• *lpcor-group*—String that identifies the LPCOR resource group.

Step 6	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits voice-service configuration mode.

Step 7	**voice lpcor policy** *lpcor-group*
	
	Example:
	`Router(cfg-lpcor-custom)#group 10 Manager`
	`Router(cfg-lpcor-custom)#group 11 LocalUser`
	`Router(cfg-lpcor-custom)#group 12 RemoteUser`
	`Router(cfg-lpcor-custom)#group 13 PSTNTrunk`
	`Router(cfg-lpcor-custom)#group 14 IPTrunk`
		Creates a LPCOR policy for a resource group.
		• *lpcor-group*—Name of the resource group that you defined in Step 5.

Step 8	**accept** *lpcor-group* **fac**
	
	Example:
	`Router(cfg-lpcor-policy)# accept PSTNTrunk fac`
	`Router(cfg-lpcor-policy)# accept Manager fac`
		Allows a LPCOR policy to accept calls associated with the specified resource group.
		• Default: Calls from other groups are rejected; calls from the same resource group are accepted.
		• fac—Valid forced authorization code that the caller needs to enter before the call is routed to its destination.
		• Repeat this command for each resource group whose calls you want this policy to accept.

Step 9	**service** *fac*	Enables force authorization code service for a LPCOR group.

	Command or Action	Purpose
	Example: `Router(cfg-lpcor-policy)#service fac`	• Default: No form of the service fac command is the default setting of a LPCOR group policy.
Step 10	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Example:

```
Router# show voice lpcor policy
voice lpcor policy PSTNTrunk (group 13):
service fac is enabled
  ( accept     ) Manager (group 10)
  ( reject     ) LocalUser (group 11)
  ( reject     ) RemoteUser (group 12)
  ( accept     ) PSTNTrunk (group 13)
  ( reject     ) IPTrunk (group 14)
```

Define Parameters for Authorization Package

To define required parameters for user name and password, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **package auth**
5. **param passwd**
6. **param user-prompt** *filename*
7. **param passwd-prompt** *filename*
8. **param max-retries**
9. **param term-digit**
10. **param abort-digit**
11. **param max-digits**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**application**
	
	Example:
	`Router(config)#application`
	`Router(config-app)#`
		Enters the application configuration mode.

Step 4	**package auth** **Example:** `Router(config-app)#package auth`	Enters package authorization configuration mode.
Step 5	**param passwd** **Example:** `Router(config-app)#package param passwd 12345`	Character string that defines a predefined password for authorization. **Note** Password digits collection is optional if password digits are predefined in the **param passwd** command.
Step 6	**param user-prompt** *filename* **Example:** `Router(config-app-param)#param user-prompt flash:en_bacd_enter_dest.au`	Allows you to enter the user name parameters required for package authorization for FAC authentication. • **user-prompt** *filename* — Plays an audio prompt requesting the caller to enter a valid username (in digits) for authorization.
Step 7	**param passwd-prompt** *filename* **Example:** `Router(config-app-param)#param passwd-prompt flash:en_welcome.au`	Allows you to enter the password parameters required for package authorization for FAC authentication. • **passwd-prompt** *filename*— Plays an audio prompt requesting the caller to enter a valid password (in digits) for authorization.
Step 8	**param max-retries** **Example:** `Router(config-app-param)#param max-retries 0`	Specifies number of attempts to re-enter an account or a password. • **max-entries—**Value ranges from 0-10, default value is 0.

	Command or Action	Purpose
Step 9	**param term-digit** **Example:** `Router(config-app-param)#param term-digit #`	Specifies digit for terminating an account or a password digit collection.
Step 10	**param abort-digit** **Example:** `Router(config-app-param)#param abort-digit *`	Specifies the digit for aborting username or password digit input. Default value is *.
Step 11	**param max-digits** **Example:** `Router(config-app-param)#param max-digits 32`	Maximum number of digits in a username or password. Range of valid value: 1 - 32. Default value is 32.
Step 12	**exit** **Example:** `Router(conf-app-param)# exit`	Exits package authorization parameter configuration mode.

Configuration Example for Forced Authorization Code

Example for Configuring Forced Authorization Code

This section provides configuration example for Forced Authorization Code.

```
!
gw-accounting aaa
!
aaa new-model
!
aaa authentication login default local
aaa authentication login h323 local
aaa authorization exec h323 local
aaa authorization network h323 local
!
aaa session-id common
!
voice lpcor enable
voice lpcor custom
group 11 LocalUser
group 12 AnalogPhone
!
voice lpcor policy LocalUser
service fac
accept LocalUser fac
accept AnalogPhone fac
!
```

```
voice lpcor policy AnalogPhone
service fac
accept LocalUser fac
accept AnalogPhone fac
!
application
package auth
 param passwd-prompt flash:en_bacd_welcome.au
 param passwd 54321
 param user-prompt flash:en_bacd_enter_dest.au
 param term-digit #
 param abort-digit *
 param max-digits 32
!
username 786 password 0 54321
!
voice-port 0/1/0
station-id name Phone1
station-id number 1235
caller-id enable
!
voice-port 0/1/1
lpcor incoming AnalogPhone
lpcor outgoing AnalogPhone
!
dial-peer voice 11 pots
destination-pattern 99329
port 0/1/1
!
ephone-dn  102  dual-line
number 786786
label HussainFAC
!
!
ephone  102
lpcor type local
lpcor incoming LocalUser
lpcor outgoing LocalUser
device-security-mode none
mac-address 0005.9A3C.7A00
type CIPC
button  1:102
```

Feature Information for Forced Authorization Code

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

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

Table 57: Feature Information for Forced Authorization Code

Feature Name	Cisco Unified CME Version	Modification
Forced Authorization Code	8.5	Introduced the FAC feature.

CHAPTER 25

Headset Auto Answer

Information About Headset Auto Answer

Auto Answering Calls Using a Headset

In Cisco Unified CME 4.0 and later versions you can configure lines on specific phones to automatically connect to incoming calls when the headset key is activated. The phone cannot be busy with an active call and the headset key must be engaged to automatically answer calls. Incoming calls are automatically answered one by one on the phone as long as the headset light remains lit. For each ephone, you can specify one or more lines for headset auto answer.

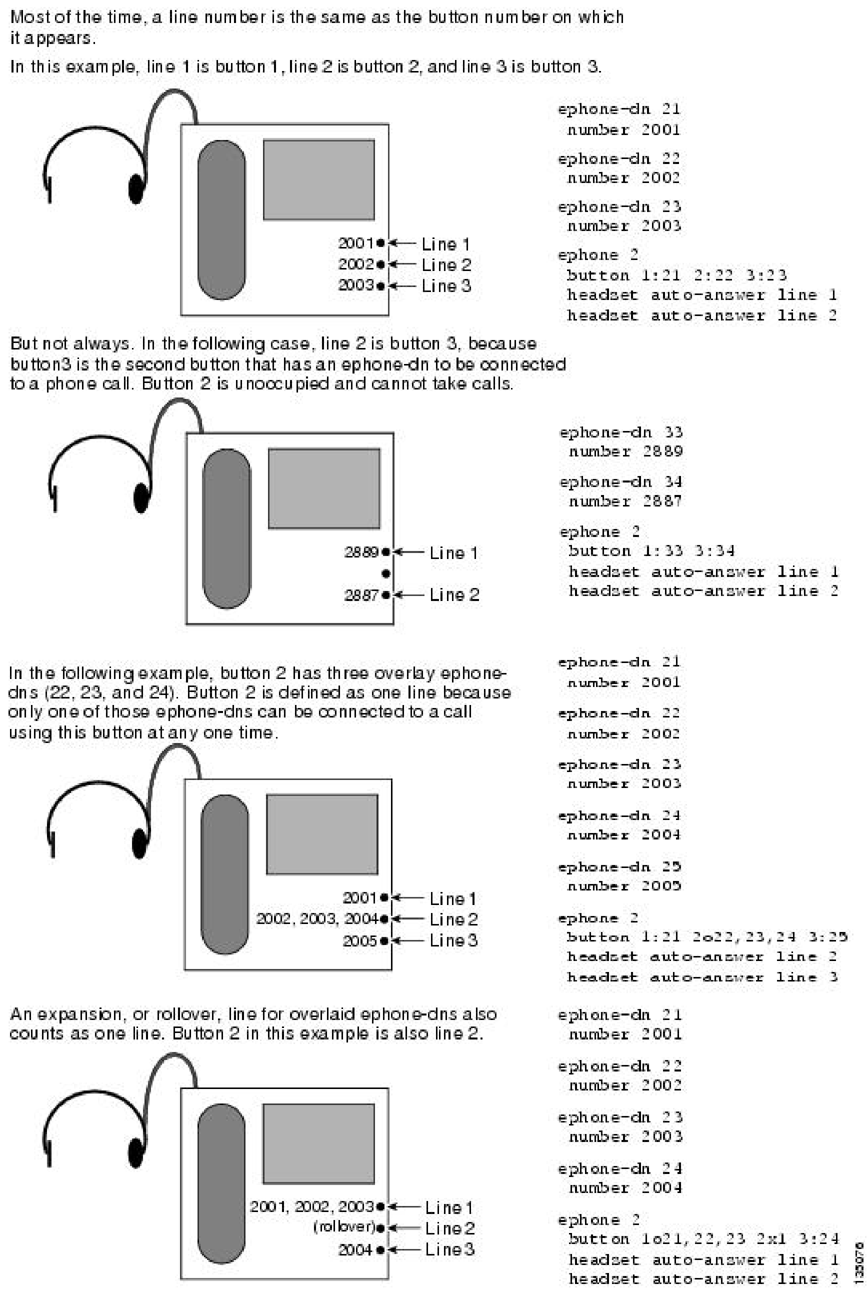
After a phone is configured for headset auto answer, the phone user must press the headset key to start auto answer. The headset light is lit to indicate that auto answer is active for the lines that are designated in the configuration. When the phone auto answers a call, a *zip* tone is played to alert the phone user that a call is present. To stop auto answer, the phone user presses the headset key again and the headset light goes out. At this time, the phone user can answer calls in a normal manner using the handset.

Difference Between a Line and a Button

Note that a line is similar to, but not exactly the same as, a button on the phone. A line represents a phone's capability to make a call connection, so each button that can make a call connection becomes a line. (For example, unoccupied buttons or speed-dial buttons are not lines.) Note also that a line is not the same as an ephone-dn. A button with overlaid ephone-dns is only one line, regardless of whether it has several ephone-dns (extension numbers) associated with it. In most cases an ephone's line numbers do match its button numbers, but in a few cases they do not.

Figure 28: When is a Line the Same as a Button?, on page 778 illustrates a comparison of line numbers and button numbers for different types of ephone configurations.

Figure 28: When is a Line the Same as a Button?



Configure Headset Auto Answer

Enable Headset Auto Answer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **headset auto-answer line** *line-number*
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** *phone-tag* **Example:** `Router(config)# ephone 25`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones for a particular Cisco Unified CME system is version- and platform-specific. For the range of values, see the CLI help.
Step 4	**headset auto-answer line** *line-number* **Example:** `Router(config-ephone)# headset auto-answer line 1`	Specifies a line on an ephone that will be answered automatically when the headset button is depressed. • *line-number*—Number of the phone line that should be automatically answered. **Note** Repeat this command to add additional lines.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verify Headset Auto Answer

Step 1 Use the **show running-config** command to verify your configuration. Headset auto answer is listed in the ephone portion of the output.

Router# **show running-config**

```
ephone  1
 headset auto-answer line 1
 headset auto-answer line 2
 headset auto-answer line 3
 headset auto-answer line 4
 username "Front Desk"
 mac-address 011F.92B0.BE03
 speed-dial 1 330 label "Billing"
 type 7960 addon 1 7914
 no dnd feature-ring
 keep-conference
 button  1f40 2f41 3f42 4:30
 button  5:405 7m20 8m21 9m22
 button  10m23 11m24 12m25 13m26
 button  14m499 15:1 16m31 17f498
 button  18s500
 night-service bell
```

Step 2 Use the **show telephony-service ephone** command to display only the ephone configuration portion of the running configuration.

Configuration Example for Headset Auto Answer

Example for Enabling Headset Auto Answer

The following example enables headset auto answer on ephone 3 for line 1 (button 1) and line 4 (button 4).

```
ephone 3
   button 1:2 2:4 3:6 4o21,22,23,24,25
   headset auto-answer line 1
   headset auto-answer line 4
```

The following example enables headset auto answer on ephone 17 for line 2 (button 2), which has overlaid ephone-dns, and line 3 (button 3), which is an overlay rollover line.

```
ephone 17
   button 1:2 2o21,22,23,24,25 3x2
```

```
   headset auto-answer line 2
   headset auto-answer line 3
```

The following example enables headset auto answer on ephone 25 for line 2 (button 3) and line 3 (button 5). In this case, the button numbers do not match the line numbers because buttons 2 and 4 are not used.

```
ephone 25
   button 1:2 3:4 5:6
   headset auto-answer line 2
   headset auto-answer line 3
```

Feature Information for Headset Auto Answer

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

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

Table 58: Feature Information for Headset Auto Answer

Feature Name	Cisco Unified CME Version	Feature Information
Headset Auto Answer	4.0	Headset auto answer was introduced.

CHAPTER 26

Intercom Lines

Information About Intercom Lines

Intercom Auto-Answer Lines

An intercom line is a dedicated two-way audio path between two phones. Cisco Unified CME supports intercom functionality for one-way and press-to-answer voice connections using a dedicated pair of intercom directory numbers on two phones that speed-dial each other.

When an intercom speed dial button is pressed, a call is speed-dialed to the directory that is the other half of the dedicated pair. The called phone automatically answers the call in speaker-phone mode with mute activated, providing a one-way voice path from the initiator to the recipient. A beep is sounded when the call is auto-answered to alert the recipient to the incoming call. To respond to the intercom call and open a two-way voice path, the recipient deactivates the mute function by pressing the Mute button or, on phones such as the Cisco Unified IP Phone 7910, lifting the handset.

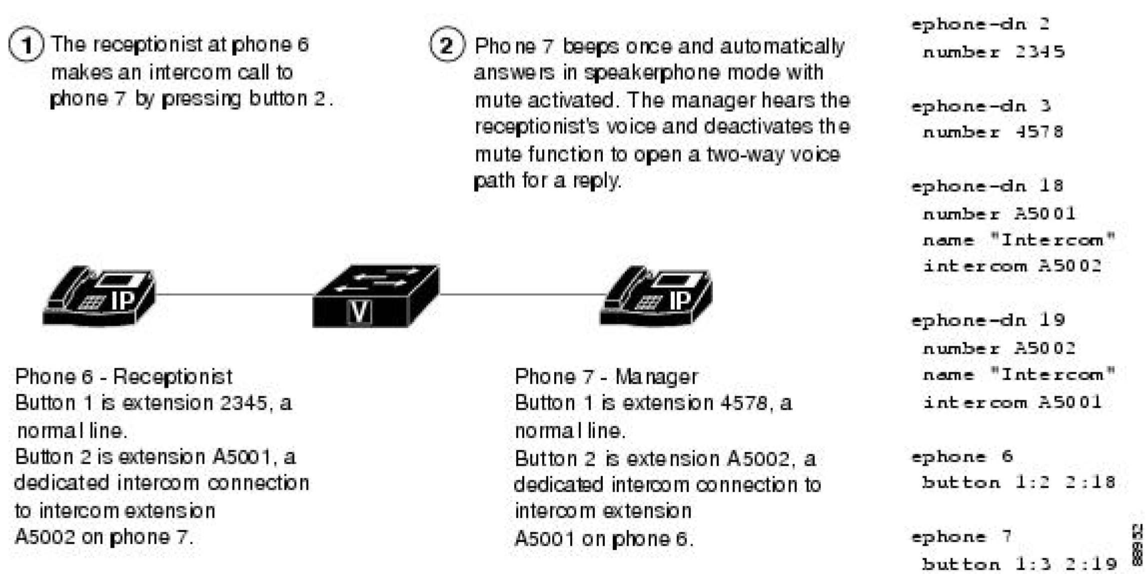
In Cisco CME 3.2.1 and later versions, you can deactivate the speaker-mute function on intercom calls. For example, if phone user 1 makes an intercom call to phone user 2, both users hear each other on connection when no-mute is configured. The benefit is that people who receive intercom calls can be heard without them having to disable the mute function. The disadvantage is that nearby background sounds and conversations can be heard the moment a person receives an intercom call, regardless of whether they are ready to take a call or not.

Intercom lines cannot be used in shared-line configurations. If a directory number is configured for intercom operation, it must be associated with one IP phone only. The intercom attribute causes an IP phone line to operate as an autodial line for outbound calls and as an autoanswer-with-mute line for inbound calls. Figure 29: Intercom Lines, on page 784 shows an intercom between a receptionist and a manager.

To prevent an unauthorized phone from dialing an intercom line (and creating a situation in which a phone automatically answers a nonintercom call), you can assign the intercom a directory number that includes an alphabetic character. No one can dial the alphabetic character from a normal phone, but the phone at the other end of the intercom can be configured to dial the number that contains the alphabetic character through the Cisco Unified CME router. For example, the intercom ephone-dns in Figure 29: Intercom Lines, on page 784 are assigned numbers with alphabetic characters so that only the receptionist can call the manager on his or her intercom line, and no one except the manager can call the receptionist on his or her intercom line.

Note An intercom requires the configuration of two ephone-dns, one each on a separate phone.

Figure 29: Intercom Lines



Whisper Intercom

When a phone user dials a whisper intercom line, the called phone automatically answers using speaker-phone mode, providing a one-way voice path from the caller to the called party, regardless of whether the called party is busy or idle.

Unlike the standard intercom feature, this feature allows an intercom call to a busy extension. The calling party can only be heard by the recipient. The original caller on the receiving phone does not hear the whisper page. The phone receiving a whisper page displays the extension and name of the party initiating the whisper page and Cisco Unified CME plays a zipzip tone before the called party hears the caller's voice. If the called party wants to speak to the caller, the called party selects the intercom line button on their phone. The lamp for intercom buttons are colored amber to indicate one-way audio for whisper intercom and green to indicate two-way audio for standard intercom.

You must configure a whisper intercom directory number for each phone that requires the Whisper Intercom feature. A whisper intercom directory number can place calls only to another whisper intercom directory number. Calls between a whisper intercom directory number and a standard directory number or intercom directory number are rejected with a busy tone.

This feature is supported in Cisco Unified CME 7.1 and later versions. For configuration information, see Configure Whisper Intercom on SCCP Phones, on page 788.

SIP Intercom

In Cisco Unified CME 8.8, the SIP Intercom feature is released as part of the 8.3(1) IP Phone firmware.

The SIP intercom line provides a one-way voice path from the caller to the called phone. When a phone user dials the intercom line, the called phone automatically answers the call in speaker-phone mode with Mute activated. If the called SIP phone is busy with a connected call or with an outgoing call that has not been connected, the call is whispered into the called phone.

As soon as the called phone auto-answers, the intercom call recipient has three options:

- Listen to the one-way audio of the intercom caller without answering.
- End the call by pressing the speaker-phone button or the EndCall softkey.
- Press the intercom button to create a two-way voice path and respond to the intercom caller.

If the called phone is busy when the intercom call arrives and a response is requested, the active call is put on hold and the outgoing call that is not connected yet is canceled before the intercom call is connected for a two-way voice path.

Note The lamp for the intercom line button displays an amber light for one-way intercom and green for a two-way voice path.

You should configure an intercom directory number to begin and end an intercom call for each phone that requires the Intercom feature. For configuration information, see Configure Intercom Call Option on SIP Phones, on page 792.

However, a standard directory number without the intercom option configured can also place an intercom call. The called phone also has the option of responding to the call by pressing the intercom line button to establish a two-way voice path with the originator without the intercom option configured.

Table 59: SIP-SCCP Interactions for the SIP Intercom Feature, on page 785 shows the supported SIP-SCCP interactions for the SIP Intercom feature.

Table 59: SIP-SCCP Interactions for the SIP Intercom Feature

Originator	Terminator	Intercom
SIP normal line	SIP intercom line	Supported
SIP intercom line	SIP intercom line	Supported
SIP normal line	SCCP whisper intercom line	Not Supported
SIP intercom line	SCCP whisper intercom line	Not Supported

Originator	Terminator	Intercom
SCCP normal line	SIP intercom line	Supported
SCCP normal line	SCCP whisper intercom line	Not Supported
SCCP whisper intercom line	SIP intercom line	Not Supported
SCCP whisper intercom line	SCCP whisper intercom line	Supported
SIP normal line	SIP normal line	Not Supported
SIP intercom line	SIP normal line	Not Supported
SCCP normal line	SIP normal line	Not Supported
SCCP intercom line	SIP normal line	Not Supported
SIP normal line	SCCP normal line	Not Supported
SIP intercom line	SCCP normal line	Not Supported
SCCP normal line	SCCP normal line	Not Supported
SCCP intercom line	SCCP normal line	Not Supported

Extension Number

The extension number of an intercom line can be included in an extension mobility user-profile or extension mobility logout-profile.

The BLF feature can define the extension number of an intercom line as a speed dial on a Cisco Unified CME phone, allowing the line status of the intercom line to be monitored.

For configuration information, see Configure Extension Mobility for SIP Phones, on page 738.

Configure Intercom Lines

Configure an Intercom Auto-Answer Line on SCCP Phones

To enable a two-way audio path between two phones, perform the following steps for each Cisco Unified SCCP IP phone at both ends of the two-way voice path.

Restriction

- Intercom lines cannot be dual-line.
- If a directory number is configured for intercom operation, it can be associated with only one Cisco Unified IP phone.
- Each phone, at both ends of the two-way voice path, requires a separate configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number*
5. **name** *name*
6. **intercom** *extension-number* [[**barge-in** [**no-mute**] | **no-auto-answer** | **no-mute**] [**label** *label*]] | **label** *label*]
7. **exit**
8. **ephone** *phone-tag*
9. **button** *button-number*: *dn-tag* [[*button-number*: *dn-tag*] ...]
10. **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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 11`	Enters ephone-dn configuration mode. • Do not use the **dual-line** keyword with this command. Intercom ephone-dns cannot be dual-line.
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number A2345`	Assigns a valid intercom number. • Using one or more alphabetic characters in an intercom number ensures that the number can only be dialed from the one other intercom number that is programmed to dial this number. The number cannot be dialed from a normal phone if it contains an alphabetic character.

	Command or Action	Purpose
Step 5	**name** *name* **Example:** `Router(config-ephone-dn)# name intercom`	Sets a name to be associated with the ephone-dn. • This name is used for caller-ID displays and also shows up in the local directory associated with the ephone-dn.
Step 6	**intercom** *extension-number* [[**barge-in** [**no-mute**] | **no-auto-answer** | **no-mute**] [**label** *label*]] | **label** *label*] **Example:** `Router(config-ephone-dn)# intercom A2346 label Security`	Defines the directory number that is speed-dialed for the intercom feature when this line is used.
Step 7	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 8	**ephone** *phone-tag* **Example:** `Router(config)# ephone 24`	Enters ephone configuration mode.
Step 9	**button** *button-number*: *dn-tag* [[*button-number*: *dn-tag*] **...**] **Example:** `Router(config-ephone)# button 1:1 2:4 3:14`	Assigns a button number to the intercom ephone-dn being configured. • Use the colon separator (**:**) between the button number and the intercom ephone-dn tag to indicate a normal ring for the intercom line.
Step 10	**end** **Example:** `Router(config)# exit`	Exits ephone configuration mode and enters privileged EXEC mode.

Configure Whisper Intercom on SCCP Phones

To enable the Whisper Intercom feature on a directory number, perform the following steps.

Restriction

- Single-line phone models, such as the Cisco Unified IP Phone 7906 or 7911, are not supported.
- Whisper intercom directory numbers can place calls only to other whisper intercom numbers.
- A directory number can be configured as either a regular intercom or a whisper intercom, not both.
- Dual-line and octo-line directory numbers are not supported as intercom lines.
- Only one intercom call, either incoming or outgoing, is allowed on the phone at one time.
- Call features are not supported on intercom calls.

Before You Begin

- Cisco Unified CME 7.1 or a later version.
- IP phones require SCCP 12.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **whisper-intercom** [**label** *string* | **speed-dial** *number* [**label** *string*]]
5. **end**
6. **show ephone-dn whisper**

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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 1`	Enters ephone configuration mode to create a directory number for a SCCP phone.
Step 4	**whisper-intercom** [**label** *string* | **speed-dial** *number* [**label** *string*]]	Enables whisper intercom on a directory number.

	Command or Action	Purpose
	Example: `Router(config-ephone-dn)# whisper intercom`	• **label** *string*—(Optional) Alphanumeric label that identifies the whisper intercom button. String can contain a maximum of 30 characters. • **speed-dial** *number*—(Optional) Telephone number to speed dial.
Step 5	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.
Step 6	**show ephone-dn whisper** **Example:** `Router# show ephone-dn whisper`	Displays information about whisper intercom ephone-dns that have been created.

The following example shows Whisper Intercom configured on extension 2004:

```
ephone-dn  24
 number 2004
 whisper-intercom label "sales"!
!
!
ephone  24
 mac-address 02EA.EAEA.0001
 button  1:24
```

Configure an Intercom Auto-Answer Line on SIP Phones

To enable the Intercom Auto-Answer feature for Cisco Unified SIP IP phones, perform the following steps for each IP phone at both ends of the two-way voice path.

Restriction

- If a directory number is configured for intercom operation, it can be associated with only one Cisco Unified IP phone.
- Each phone, at each end of the two-way voice path, requires a separate configuration.

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **auto-answer**
6. **exit**
7. **voice register pool** *pool-tag*
8. **id** {**mac** *address*}
9. **type** *phone-type*
10. **number** *tag* **dn** *dn-tag*
11. **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 register dn** *dn-tag* **Example:** `Router(config-register-global)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a Cisco Unified SIP IP phone, intercom line, voice port, or an MWI.
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number A5001`	Defines a valid number for the directory number being configured. • To prevent non-intercom originators from manually dialing an intercom destination, the number string can contain alphabetic characters enabling the number to be dialed only by the Cisco Unified CME router and not from telephone keypads.
Step 5	**auto-answer** **Example:** `Router(config-register-dn)# auto-answer`	Enables the Intercom Auto-Answer feature on the directory number being configured.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-register-dn)# exit`	Exits voice register dn configuration mode.
Step 7	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a Cisco Unified SIP IP phone in Cisco Unified CME.
Step 8	**id** {**mac** *address*} **Example:** `Router(config-register-pool)# id mac 0009.A3D4.1234`	Explicitly identifies a locally available individual Cisco Unified SIP IP phone to support a degree of authentication.
Step 9	**type** *phone-type* **Example:** `Router(config-register-pool)#` **type** `7960-7940`	Defines a phone type for the Cisco Unified SIP IP phone being configured.
Step 10	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 17`	Associates a directory number with the Cisco Unified SIP IP phone being configured.
Step 11	**end** **Example:** `Router(config-register-pool)# end`	Exits voice register pool configuration mode and enters privileged EXEC mode.

Configure Intercom Call Option on SIP Phones

Restriction

- The Intercom feature is not supported on single-line phones because the intercom line cannot be the primary line of a Cisco Unified CME SIP IP phone.
- The intercom line cannot be shared among SIP phones.
- FAC is not supported on a SIP intercom call because the keys are disabled.

Before You Begin

- Cisco Unified CME 8.8 or a later version.
- 8.3(1) phone firmware or a later version is installed on the Cisco Unified SIP IP phone.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **intercom** [**speed-dial** *digit-string*] [**label** *label-text*]
6. **exit**
7. **voice register pool** *pool-tag*
8. **id** {**network** *address* **mask** *mask* | **ip** *address* **mask** *mask* | **mac** *address*}
9. **type** *phone-type*
10. **number** *tag* **dn** *dn-tag*
11. **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 register dn** *dn-tag* **Example:** `Router(config)# voice register dn 4`	Enters voice register dn configuration mode to define an extension for a SIP intercom line.
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 4001`	Associates a telephone or extension number with a Cisco Unified SIP phone in a Cisco Unified CME system.
Step 5	**intercom** [**speed-dial** *digit-string*] [**label** *label-text*]	Enables the intercom call option on a Cisco Unified SIP IP phone. • (Optional) **speed-dial—**Enables the intercom line user to place a call to a pre-configured destination. If the speed dial

	Command or Action	Purpose
	Example: `Router(config-register-dn)# intercom [speed-dial 4002] [label intercom4001]`	is not configured, it simply initiates a new call on the intercom line and waits for the user to dial the destination number. • (Optional) **label** *label-text*—String that contains identifying text to be displayed next to the speed dial button. Enclose the string in quotation marks if the string contains a space.
Step 6	**exit** **Example:** `Router(config-register-dn)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 7	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a Cisco Unified SIP phone in Cisco Unified CME.
Step 8	**id** {**network** *address* **mask** *mask* | **ip** *address* **mask** *mask* | **mac** *address*} **Example:** `Router(config-register-pool)# id mac 0009.A3D4.`	Explicitly identifies a locally available individual Cisco Unified SIP phone to support a degree of authentication.
Step 9	**type** *phone-type* **Example:** `Router(config-register-pool)#` **type** `7940`	Defines a phone type for the Cisco Unified SIP phone being configured.
Step 10	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 17`	Associates a directory number tag with the Cisco Unified SIP IP phone being configured.
Step 11	**end** **Example:** `Router(config-register-dn)# end`	Exits to privileged EXEC mode.

Configuration Examples for Intercom Lines

Example for Configuring Intercom Lines

The following example shows an intercom between two Cisco Unified IP phones. In this example, ephone-dn 2 and ephone-dn 4 are normal extensions, while ephone-dn 18 and ephone-dn 19 are set as an intercom pair. Ephone-dn 18 is associated with line button 2 on Cisco Unified IP phone 4. ephone-dn 19 is associated with line button 2 on Cisco Unified IP phone 5. The two ephone-dns provide a two-way intercom between the two Cisco Unified IP phones.

```
ephone-dn 2
 number 5333

ephone-dn 4
 number 5222

ephone-dn 18
 number 5001
 name “intercom”
 intercom 5002 barge-in

ephone-dn 19
 name “intercom”
 number 5002
 intercom 5001 barge-in

ephone 4
 button 1:2 2:18

ephone 5
 button 1:4 2:19
```

Example for Configuring SIP Intercom Support

The following example shows SIP Intercom configured on extension 1001:

```
voice register dn 1
 number 1001
 intercom [speed-dial 1002] [label intercom1001]

voice register pool 1
 id mac 001D.452D.580C
 type 7962
 number 1 dn 2
 number 2 dn 1
```

Where to Go Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Paging

The paging feature sets up a one-way audio path to deliver information to a group of phones at one time. For more information, see Paging, on page 857.

Feature Information for Intercom Lines

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

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

Table 60: Feature Information for Intercom Lines

Feature Name	Cisco Unified CME Version	Feature Information
SIP Intercom	8.8	Adds intercom support to Cisco Unified SIP IP phones connected to a Cisco Unified CME system.
Whisper Intercom	7.1	Introduces whisper intercom feature.
Intercom Lines	3.4	Adds intercom feature, with no-mute function, for supported Cisco Unified IP phones that are connected to a Cisco Unified CME router and running SIP.
	3.2.1	Introduces the no-mute function.
	2.0	Introduces the Intercom feature.

CHAPTER 27

Loopback Call Routing

Information About Loopback Call Routing

Loopback Call Routing

Loopback call routing in a Cisco Unified CME system is provided through a mechanism called loopback-dn, which provides a software-based limited emulation of back-to-back physical voice ports connected together to provide a loopback call-routing path for voice calls.

Loopback call routing and loopback-dn restricts the passage of call-transfer and call-forwarding supplementary service requests through the loopback. Instead of passing these requests through, the loopback-dn mechanism attempts to service the requests locally. This allows loopback-dn configurations to be used in call paths where one of the external devices does not support call transfer or call forwarding (Cisco-proprietary or H.450-based). Control messages that request call transfer or call forwarding are intercepted at the loopback virtual port and serviced on the local voice gateway. If needed, this mechanism creates VoIP-to-VoIP call-routing paths.

Loopback call routing may be used for routing H.323 calls to Cisco Unity Express. For information on configuring Cisco Unity Express, see the Cisco Unity Express documentation.

Note A preferred alternative to loopback call routing was introduced in Cisco CME 3.1. This alternative blocks H.450-based supplementary service requests by using the following Cisco IOS commands: **no supplementary-service h450.2**, **no supplementary-service h450.3**, and **supplementary-service h450.12**. For more information, see Configure Call Transfer and Forwarding, on page 1178.

Use of loopback-dn configurations within a VoIP network should be restricted to resolving critical network interoperability service problems that cannot otherwise be solved. Loopback-dn configurations are intended for use in VoIP network interworking where the alternative would be to make use of back-to-back-connected physical voice ports. Loopback-dn configurations emulate the effect of a back-to-back physical voice-port arrangement without the expense of the physical voice-port hardware. Because digital signal processors (DSPs) are not involved in loopback-dn arrangements, the configuration does not support interworking or transcoding between calls that use different voice codecs. In many cases, use of back-to-back physical voice ports that do involve DSPs to resolve VoIP network interworking issues is preferred, because it introduces fewer restrictions in terms of supported codecs and call flows.

Loopback call routing requires two extensions (ephone-dns) to be separately configured, each as half of a loopback-dn pair. Ephone-dns that are defined as a loopback-dn pair can only be used for loopback call routing. In addition to defining the loopback-dn pair, you must specify preference, huntstop, class of restriction (COR), and translation rules.

Configure Loopback Call Routing

Enable Loopback Call Routing

To enable loopback call-routing, perform the following steps for each ephone-dn that is part of the loopback-dn pair.

Restriction Loopback-dns do not support T.38 fax relay.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **caller-id** {**local** | **passthrough**}
6. **no huntstop**
7. **preference** *preference-order* [**secondary** *secondary-order*]
8. **cor** {**incoming** | **outgoing**} *cor-list-name*
9. **translate** {**called** | **calling**} *translation-rule-tag*
10. **loopback-dn** *dn-tag* [**forward** *number-of-digits* | **strip** *number-of-digits*] [**prefix** *prefix-digit-string*] [**suffix** *suffix-digit-string*] [**retry** *seconds*] [**auto-con**] [**codec** {**g711alaw** | **g711ulaw**}]
11. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 15`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. Range is platform- and version-dependent. **Note** Ephone-dns used for loopback cannot be dual-line ephone-dns.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 2001`	Associates a number with this extension (ephone-dn). • *number*—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn. • **secondary**—(Optional) Allows you to associate a second telephone number with an ephone-dn. • **no-reg**—(Optional) Specifies that this number should not register with the H.323 gatekeeper. The **no-reg** keyword indicates that only the secondary number should not register. The **no-reg both** keywords indicate that both numbers should not register, and the **no-reg primary** keywords indicate that only the primary number should not register.
Step 5	**caller-id** {**local** | **passthrough**} **Example:** `Router(config-ephone-dn)# caller-id local`	Specifies caller-ID treatment for outbound calls originated from the ephone-dn. The default if this command is not used is as follows. For transferred calls, caller ID is provided by the number and name fields from the outbound side of the loopback-dn. For forwarded calls, caller ID is provided by the original caller ID of the incoming call. Settings for the **caller-id block** command and translation rules on the outbound side are executed. • **local**—Passes the local caller ID on redirected calls. This is the preferred usage. • **passthrough**—Passes the original caller ID on redirected calls.
Step 6	**no huntstop** **Example:** `Router(config-ephone-dn)# no huntstop`	Disables huntstop and allows call hunting behavior for an extension (ephone-dn).
Step 7	**preference** *preference-order* [**secondary** *secondary-order*] **Example:** `Router(config-ephone-dn)# preference 1`	Sets dial-peer preference for an extension (ephone-dn). • *preference-order*—Preference order for the primary number associated with an extension (ephone-dn). Range is 0 to 10, where 0 is the highest preference and 10 is the lowest preference. Default is 0.

	Command or Action	Purpose
		• **secondary** *secondary-order*—(Optional) Preference order for the secondary number associated with the ephone-dn. Range is 0 to 10, where 0 is the highest preference and 10 is the lowest preference. Default is 9.
Step 8	**cor** {**incoming** | **outgoing**} *cor-list-name* **Example:** `Router(config-ephone-dn)# cor incoming corlist1`	Applies a class of restriction (COR) to the dial peers associated with an extension. COR specifies which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list. For information about COR, see Dial Peer Configuration on Voice Gateway Routers.
Step 9	**translate** {**called** | **calling**} *translation-rule-tag* **Example:** `Router(config-ephone-dn)# translate called 1`	Selects an existing translation rule and applies it to a calling number or a number that has been called. This command enables the manipulation of numbers as part of a dial plan to manage overlapping or nonconsecutive numbering schemes. • **called**—Translates the called number. • **calling**—Translates the calling number. • *translation-rule-tag*—Unique sequence number of the previously defined translation rule. Range is 1 to 2147483647. **Note** This command requires that you have previously defined appropriate translation rules using the **voice translation-rule** and **rule** commands.
Step 10	**loopback-dn** *dn-tag* [**forward** *number-of-digits* | **strip** *number-of-digits*] [**prefix** *prefix-digit-string*] [**suffix** *suffix-digit-string*] [**retry** *seconds*] [**auto-con**] [**codec** {**g711alaw** | **g711ulaw**}] **Example:** `Router(config-ephone-dn)# loopback-dn 24 forward 15 prefix 415353....`	Enables H.323 call transfer and call forwarding by using hairpin call routing for VoIP endpoints that do not support Cisco-proprietary or H.450-based call-transfer and call-forwarding. • *dn-tag*—Unique sequence number that identifies the ephone-dn that is being paired for loopback with the ephone-dn that is being configured. The paired ephone-dn must be one that is already defined in the system. • **forward** *number-of-digits*—(Optional) Number of digits in the original called number to forward to the other ephone-dn in the loopback-dn pair. Range is 1 to 32. Default is to forward all digits. • **strip** *number-of-digits*—(Optional) Number of leading digits to be stripped from the original called number before forwarding to the other ephone-dn in the loopback-dn pair. Range is 1 to 32. Default is to not strip any digits. • **prefix** *prefix-digit-string*—(Optional) Defines a string of digits to add in front of the forwarded called number. Maximum number of digits in the string is 32. Default is that no prefix is defined. • **suffix** *suffix-digit-string*—(Optional) Defines a string of digits to add to the end of the forwarded called number. Maximum number of digits in the string is 32. Default is that no suffix is defined. If you add a suffix that starts with the pound character (#), the string must be enclosed in quotation marks.

	Command or Action	Purpose
		• **retry** *seconds*—(Optional) Number of seconds to wait before retrying the loopback target when it is busy or unavailable. Range is 0 to 32767. Default is that retry is disabled and appropriate call-progress tones are passed to the call originator. • **auto-con**—(Optional) Immediately connects the call and provides in-band alerting while waiting for the far-end destination to answer. Default is that automatic connection is disabled. • **codec**—(Optional) Explicitly forces the G.711 A-law or G.711 mu-law voice coding type to be used for calls that pass through the loopback-dn. This overrides the G.711 coding type that is negotiated for the call and provides conversion from mu-law to A-law, if needed. Default is that Real-Time Transport Protocol (RTP) voice packets are passed through the loopback-dn without considering the G.711 coding type negotiated for the calls. • **g711alaw**—G.711 A-law, 64000 bits per second, for T1. • **g711ulaw**—G.711 mu-law, 64000 bits per second, for E1.
Step 11	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged exec mode.

Verify Loopback Call Routing

Use the **show running-config** or **show telephony-service ephone-dn** command to display ephone-dn configurations.

Configuration Example for Loopback Call Routing

Example for Enabling Loopback Call Routing

The following example uses ephone-dns 15 and 16 as a loopback-dn pair. Calls are routed through this loopback ephone-dn pair in the following way:

- An incoming call to 4085552xxx enters the loopback pair through ephone-dn 16 and exits the loopback via ephone-dn 15 as an outgoing call to 2xxx (based on the forward 4 digits setting).

- An incoming call to 6xxx enters the loopback pair through ephone-dn 15 and exits the loopback via ephone-dn 16 as an outgoing call to 4157676xxx (based on the prefix 415767 setting).

```
ephone-dn 15
   number 6...
   loopback-dn 16 forward 4 prefix 415767
   caller-id local
   no huntstop
  !
  ephone-dn 16
   number 4085552...
   loopback-dn 15 forward 4
   caller-id local
   no huntstop
```

Feature Information for Loopback Call Routing

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

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

Table 61: Feature Information for Loopback Call Routing

Feature Name	Cisco Unified CME Version	Feature Information
Loopback Call Routing	2.0	Loopback call routing was introduced.

CHAPTER 28

Multilevel Precedence and Preemption

This document describes the Multilevel Precedence and Preemption (MLPP) service introduced in Cisco Unified Communications Manager Express 7.1 (Cisco Unified CME).

Prerequisites for MLPP

- Cisco Unified CME 7.1
- Cisco IOS Release 12.4(24)T
- To use Cisco Unified CME basic automatic call distribution (B-ACD) and auto-attendant (AA) service as the MLPP attendant-console application, you must download and install the B-ACD scripts. These scripts are available from the Cisco Unified CME Software Download site at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.
- You can use your own audio files for the blocked precedence announcement and busy station not equipped for preemption announcement or you can use the audio files available from the Cisco Unified CME Software Download site at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Information About MLPP

Multilevel Precedence and Preemption (MLPP) service allows validated users to place priority calls, and if necessary, to preempt lower-priority calls. Precedence indicates the priority level of a call. Preemption is the process of terminating a lower-precedence call so a call of higher precedence can proceed. This capability assures high-ranking personnel can communicate with critical organizations and personnel during network stress situations, such as a national emergency or degraded network situation.

Precedence

Precedence indicates the priority level associated with an MLPP call. Phone users can apply a precedence level when making a call.

You define an MLPP access digit in Cisco Unified CME and assign a maximum precedence level to individual phones. Phone users request a precedence call by dialing the access code NP, where N specifies the pre-configured access digit and P specifies the requested precedence level, followed by the phone number.

Table 62: DSN Precedence Levels lists the precedence levels that can be associated with an MLPP call in the Defense Switched Network (DSN) domain.

Table 62: DSN Precedence Levels

Level	Precedence
0 (high)	Flash Override
1	Flash
2	Immediate
3	Priority
4 (low)	Routine

Table 63: DRSN Precedence Levels lists the precedence levels that can be associated with an MLPP call in the Defense Red Switched Network (DRSN) domain.

Table 63: DRSN Precedence Levels

Level	Precedence
0 (high)	Flash Override Override
1	Flash Override
2	Flash
3	Immediate
4	Priority
5 (low)	Routine

A precedence call is any call with a precedence level higher than Routine. If precedence is not specifically invoked, the system processes a call using normal call processing and call forwarding.

Emergency 911 calls are automatically assigned precedence level 0.

Cisco Unified CME provides precedence indications to the source and destination of a precedence call, respectively, if either has MLPP indication enabled. For the source, this indication includes a precedence ringback tone and display of the precedence level of the call, if the device supports display. For the destination, the indication includes a precedence ringer tone and display of the precedence level of the call, if the device supports display.

Basic Precedence Call Setup

The following sequence of events occurs during the setup of a precedence call:

1. Phone user goes off hook and dials a precedence call. The call pattern is NP-xxxx, where N is the precedence access digit, P is the precedence level for the call, and xxx is the extension or phone number of the called party.
2. The calling party receives the precedence ringback tone and the precedence display while the call is processing.
3. The called party receives the precedence ringer tone and the precedence display that indicates the precedence call.

Example

Party 1000 makes a precedence call to party 1001. To do so, party 1000 dials the precedence call pattern, such as 80-1001.

While the call processes, the calling party (1000) receives the precedence ringback tone and precedence display on their Cisco Unified IP Phone. After acknowledging the precedence call, the called party (1001) receives a precedence ringer tone and a precedence display on their Cisco Unified IP Phone.

Preemption

Preemption is the process of terminating an active call of lower precedence so a call of higher precedence can proceed. Preemption includes the notification and acknowledgment of preempted users and the reservation of shared resources immediately after preemption and before call termination. Preemption can take one of the following two forms:

- User Access Preemption—This type of preemption applies to phones and other end-user devices. If a called party is busy with a lower precedence call, both the called party and the party to which it is connected, receive preemption notification and the existing call is cleared immediately.

  For calls to Cisco Unified IP phones, the called party can hang up immediately to connect to the new higher precedence call, or if the called party does not hang up, Cisco Unified CME forces the phone on-hook after the configured preemption tone timer expires and connects the call.

  For FXS ports, the called party must acknowledge the preemption by going on-hook, before being connected to the new higher precedence call.

- Common Network Facility Preemption—This type of preemption applies to trunks. If all channels of a PRI trunk are busy with calls of lower precedence, a call of lower precedence is preempted to complete the higher precedence call.

  Cisco Unified CME selects a trunk by first searching for an idle channel on all corresponding trunks (based on matching the called number in the dial peer).

If an idle channel is not found, Cisco Unified CME performs a preemptive-search by searching one trunk at a time for an idle channel. If no idle-channel is available on a trunk, preemption is performed on the lowest of lower-precedence calls corresponding to the trunk. If none of the calls corresponding to the trunk is of lower precedence, the next trunk is searched and so on.

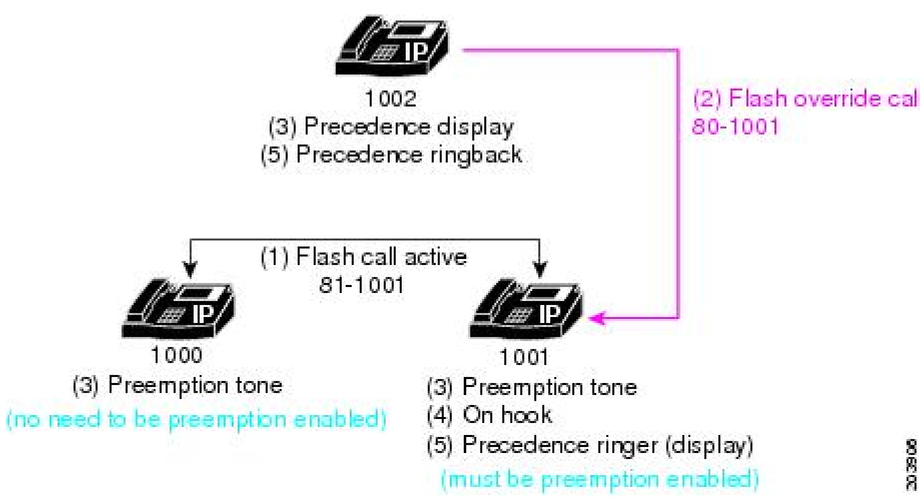
SCCP phones support up to eight calls per directory number. When all lines are busy and a higher precedence MLPP call comes in, Cisco Unified CME preempts a lower precedence call on one of the channels of the directory number.

The maximum precedence level that a user can assign to an MLPP call originating from a specific phone is set using ephone templates and applied to individual phones. Calls from directory numbers that are shared by SCCP phones can have different maximum precedence levels, based on the precedence level of the phone.

Basic Preemption Call

Figure 30: User Access Preemption Example shows an example of user access preemption.

Figure 30: User Access Preemption Example



In this example, the following sequence of events occurs:

1. User 1000 places a call with precedence level 1 (flash) to user 1001, and preemption is enabled for user 1001. In this example, user 1000 dials 81-1001 to place the precedence call.
2. User 1002 places a precedence call to user 1001 by dialing 80-1001. This call, which is of precedence level 0 (flash override), is a higher precedence call than the active precedence call.
3. Phone 1002 receives precedence display (flash override display), and the phones that are involved in the existing lower precedence call both play preemption tones (users 1000 and 1001).
4. To complete preemption, the parties who are involved in the lower precedence call hang up (users 1000 and 1001).
5. The higher level precedence call is offered to user 1001, who receives a precedence ringer tone (if MLPP indication is enabled). The calling party, user 1002, receives precedence ringback.

DSN Dialing Format

Cisco Unified CME 8.0 and later releases provide complete support of the DSN dialing format, as outlined in Table 64: DSN Dialing Format.

Table 64: DSN Dialing Format

[Access-digit {Precedence-level |Service-digit}]			[Route-code]	[Area-code]	Switch-code	Line-number
[N {P | S}]			[1X]	[KXX]	KXX	XXXX
N is 2 - 9	P is 0 - 4	S is 5 - 9	X is 0 - 9	K is 2 - 8		

Service Digit

The service digit provides information to the switch for connecting calls to government or public telephone services or networks. The services are reached through the trunk or route that is selected based on the dialed digits. Phone users request a service by dialing the access code NS, where N specifies the pre-configured access digit and S specifies the requested service, followed by the phone number.

Table 65: Service Digit lists the service digits supported in Cisco Unified CME 8.0 and later versions.

Table 65: Service Digit

Service Digit	Precedence
5	Off-net 700 services
6	Not assigned
7	DSN CONUS FTS
8	Not assigned
9	Local PSTN

In Cisco Unified CME, the route pattern is configured to supply secondary dial-tone and the remainder of the digits are collected and passed to the PSTN trunk as the called number. The digits that follow the access digit and service digit must be NANP compliant (E.164 number).

Cisco Unified CME provides secondary dial tone after the two digits and then routes the call based on the remaining collected digits (using the dial plan configuration). These services are assumed to be reached through the trunk (or route) selected based on the dialed digits (dialed after the route digits).

Route Code

The route code allows a phone user to inform the switch of special routing or termination requirements. The route code determines whether a call uses circuit-switched data or voice-grade trunking and can be used to disable echo suppressors and cancellers, and override satellite link control.

The first digit of the route code is 1. It is a required part of the dialing plan to inform the switch that the next digit, the route digit, provides network instructions for specialized routing. Phone users dial route codes in the form 1X, where X is the route digit. The supported route digits that a user can dial are 0 and 1.

Table 66: Route Codes lists the route codes supported in Cisco Unified CME 8.0 and later versions:

Table 66: Route Codes

Route Code	Use	Description
10	Voice call (default)	Any codec that carries voice or voice band data, such as G.711, G.729, or fax or modem pass-through.
11	Circuit-switched data	Any codec that carries unaltered DS0 traffic over IP (circuit emulation). For Cisco Unified CME, this is the audio/clearmode codec (RFC-4040).

Example for Dialing

If the first digit that the user dials is the configured access digit, this indicates an access code where the next digit is either a precedence digit or a service digit. If the next digit dialed is:

- 0-4—This is a precedence call. Cisco Unified CME sets the precedence indication, stores the precedence value, and discards the digits.
- 5-9—This is a call to a particular service. Cisco Unified CME passes the call to the designated trunk, discards the digits, and plays secondary dial tone.

If the first digit that the user dials or the next digit dialed after the access code is:

- 1—This is a route code and the next digit is a route digit. The supported route digits that a user can dial are 0 and 1. Cisco Unified CME stores the route code for use later in route selection, sets a trunk-type indication, and discards the route code digits.

If the first digit that the user dials or the next digit dialed after the access code or route code is:

- 2-8—This is the first digit of the area code or switch code. Area codes and switch codes in the DSN are allocated so there is no overlap. The area code and/or switch code are used for route selection.

MLPP Service Domains

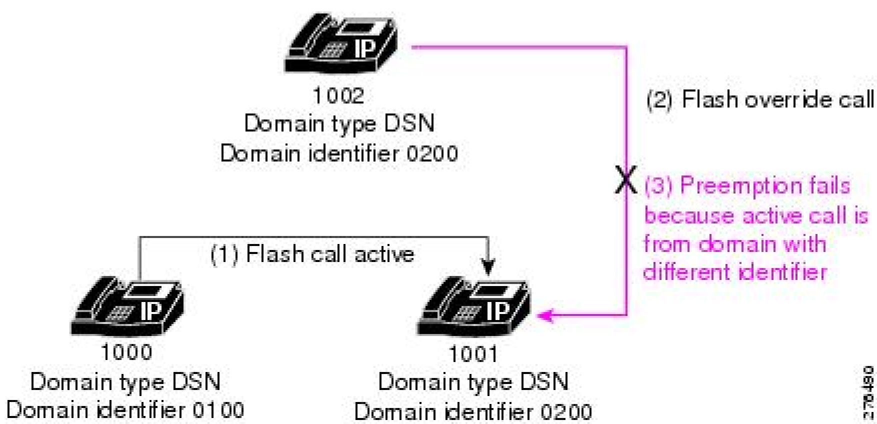
Cisco Unified CME 8.0 and later versions support MLPP service domains. A service domain consists of a group of MLPP subscribers and network resources. Calls and resources can only be preempted by higher-priority calls from MLPP subscribers within the same domain.

You can configure each device with a domain type, such as DSN or DRSN, and a domain identifier. You can assign a global MLPP domain type and identifier to the Cisco Unified CME router and assign different service domains to the individual phones registered to Cisco Unified CME through an ephone template. Calls from any phone that is not configured with a specific service domain use the global domain type and identifier.

The MLPP precedence and preemption applies only within the same domain. Only calls within the same domain can be preempted. If a call is placed between two subscribers with different MLPP service domains, Cisco Unified CME assigns the service domain of the originator to the call.

Figure 31: Service Domains with Different identifiers shows an example of preemption attempted across domains with different identifier numbers.

Figure 31: Service Domains with Different identifiers



In the example shown in Figure 31: Service Domains with Different identifiers, the following sequence of events occurs:

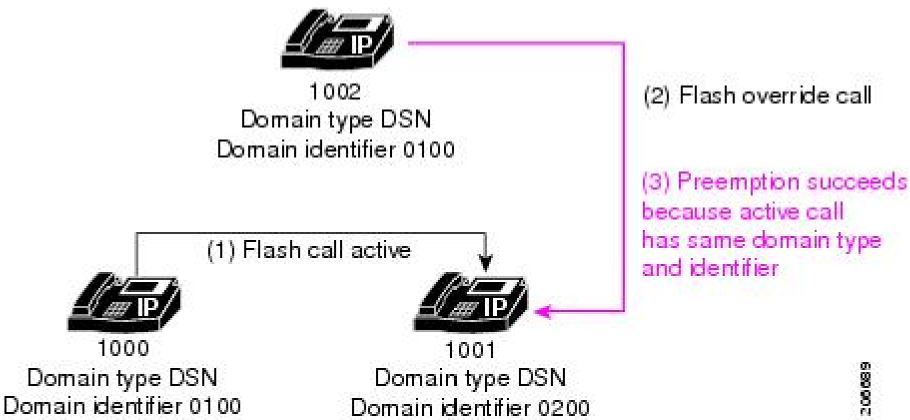
1. User 1000, from service domain 0100, places a call with precedence level 1 (flash) to user 1001 in service domain 0200. The call is assigned domain number 0100 because that is the service domain of the call originator.
2. User 1002, from domain number 0200, places a precedence call to user 1001. This call, which is of precedence level 0 (flash override), is a higher precedence call than the active precedence call.
3. The active call is not preempted because the incoming call is from a different service domain than the active call; a call from domain 0200 cannot preempt a call from domain 0100.

In the example shown in Figure 32: Service Domains with Different Domain Types, the active call is not preempted because the incoming call is from a different domain type than the active call; a call from the DSN cannot preempt a call from the DRSN.

Figure 32: Service Domains with Different Domain Types

In the example shown in Figure 33: Service Domains with Same Type and identifier, the active call is successfully preempted because the incoming call has the same domain type and identifier as the active call.

Figure 33: Service Domains with Same Type and identifier



MLPP Indication

For basic MLPP calls with MLPP indication enabled, Cisco Unified CME instructs SCCP phones to play the precedence ringer tone and display the precedence level.

For basic MLPP calls with preemption involved and MLPP indication enabled, Cisco Unified CME instructs both parties to play the preemption tone and display the precedence level of the MLPP call on the phone.

For an MLPP call with call waiting, if MLPP indication is enabled, Cisco Unified CME instructs SCCP phones to play priority the call waiting tone instead of the regular call waiting tone.

Users receive an error tone if they attempt to make a call with a higher level of precedence than the highest precedence level that is authorized for their phone.

For example, user 1002 dials 80 to start a precedence call. Eight (8) represents the precedence access digit, and zero (0) specifies the precedence level that the user attempts to use. If this user is not authorized to make level 0 (flash override) precedence calls, the user receives an error tone.

MLPP Announcements

Users who are unable to place MLPP calls receive announcements that detail the reasons why a call was unsuccessful. Table 67: MLPP Announcements lists the supported MLPP announcements.

Table 67: MLPP Announcements

Announcement	Condition
Blocked Precedence Announcement (BPA)	
(Switch name and Location). Equal or higher precedence calls have prevented completion of your call. Please hang up and try again. This is a recording. (Switch name and Location).	An equal or higher precedence call is in progress.
	Users receive the BPA if the destination party for the precedence call is off hook or if the destination party is busy with a precedence call of an equal or higher precedence. BPA is not played if the destination party is configured for Call Waiting or Call Forwarding, or uses automatic call diversion to an attendant-console service. Supported in Cisco Unified CME 7.1 and later versions.
Busy Not Equipped Announcement (BNEA)	
(Switch name and Location). A service disruption has prevented the completion of your call. Please wait 30 minutes and try again. In case of emergency call your operator. This is a recording. (Switch name and Location).	Busy station not equipped for preemption.
	Users receive the BNEA if the dialed number is busy and non-preemptable. BNEA is not played if the dialed number is configured for Call Waiting or Call Forwarding, or has alternate party designations. Supported in Cisco Unified CME 7.1 and later versions.
Isolated Code Announcement (ICA)	
(Switch name and Location). A service disruption has prevented the completion of your call. Please wait 30 minutes and try again. In case of emergency call your operator. This is a recording. (Switch name and Location).	Operating or equipment problems encountered.
	The complete trunk group including all routes is busied manually at either end of the circuit or the complete trunk group including all routes is in a carrier group alarm state (for example, Loss of Signal, Remote Alarm Indication, or Alarm Indication Signal). Supported in Cisco Unified CME 8.0 and later versions.
Loss of C2 Features Announcement (LOC2)	

Announcement	Condition
-	Call leaves DSN.
	Users receive the LOC2 announcement when the call leaves the Cisco Unified CME router on the trunk or when the user places a call to a different domain. For example, DSN callers who place calls to locations that permit off-net terminations may receive an announcement informing them that they have left the DSN. Supported in Cisco Unified CME 8.0 and later versions.
Unauthorized Precedence Level Announcement (UPA)	
(Switch name and Location). The precedence used is not authorized for your line. Please use an authorized precedence or ask your attendant for assistance. This is a recording. (Switch name and Location).	Unauthorized precedence level is attempted.
	Users receive the UPA when they attempt to make a precedence call by using a higher level of precedence than the highest precedence level that is authorized for their line. Supported in Cisco Unified CME 8.0 and later versions.
Vacant Code Announcement (VCA)	
(Switch name and Location). Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording. (Switch name and Location).	No such service or invalid code.
	Users receive the VCA when they dial an invalid or unassigned number. Supported in Cisco Unified CME 8.0 and later versions.

Automatic Call Diversion (Attendant Console)

Cisco Unified CME supports automatic diversion of all unanswered precedence calls above Routine to a designated directory number or attendant console after a selected period of time.

If automatic call diversion of MLPP calls is configured in Cisco Unified CME, it overrides the Call Forward settings on the phone for all incoming precedence calls above Routine and forwards these calls to the attendant-console application specified in the MLPP configuration. Cisco Unified CME treats MLPP calls with a precedence level of Routine as normal calls and honors the Call Forward setting configured on the phone.

How Cisco Unified CME handles forwarded MLPP calls depends on the following Call Forward options:

- Call Forward All (CFA)—Precedence calls are routed to the target number of the attendant console immediately. The CFA target is not used for MLPP calls.
- Call Forward Busy (CFB)—Precedence calls are forwarded to the configured CFB destination. If the CFB destination is Voice Mail or an off-net endpoint, the call is forwarded to the target number of the attendant-console service.
- Call Forward No Answer (CFNA)—Precedence calls are forwarded to the configured CFNA destination. If the CFNA destination does not answer before the CFNA timer expires, or it is voice mail or an off-net endpoint, the call is forwarded to the target number of the attendant-console service.

Calls diverted to the attendant console are indicated by a visual signal and placed in the queue for attendant service by precedence and time interval. The call with the highest precedence and longest holding time is answered first. Attendant Queue Announcement is played to calls waiting in the queue for attendant service. Call distribution is performed to reduce excessive waiting time and each attendant position operates from a common queue. Cisco Unified CME supports attendant console service for MLPP using Basic Automatic Call Distribution (B-ACD) and auto-attendant (AA) service.

Configure MLPP

Enable MLPP Service Globally in Cisco Unified CME

This task covers the basic steps necessary to enable MLPP on the router.

Restriction

- SIP phones are not supported.
- Cisco Unified IP Phone 6900 Series phones are not supported.
- Cisco Unified CME in SRST Fallback mode is not supported.
- Supports only ISDN PRI E1 and T1interfaces.
- Supports MLPP service within the local Cisco Unified CME router only.
- Cisco Unified CME 7.1 supports only Basic Calls, Call Forward, Call Hold and Resume, Consultative Call-Transfer, and Call Waiting. Blind Transfer is not supported.
- Cisco Unified CME 8.0 and later versions support Three-Party Ad Hoc Conferencing and Call Pickup.
- Call Park Retrieval based on precedence level is not supported; Cisco Unified CME must be configured to accept only one call per park slot.

Before You Begin

Trunks must belong to a trunk group and have preemption enabled. For configuration information, see Enabling Preemption on the Trunk Group in *Integrating Data and Voice Services for ISDN PRI Interfaces on Multiservice Access Routers*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice mlpp**
4. **access-digit** *digit*
5. **bnea** *audio-url*
6. **bpa** *audio-url*
7. **upa** *audio-url*
8. **service-domain** { **drsn** | **dsn**}**identifier** *domain-number*
9. **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 mlpp** **Example:** `Router(config)# voice mlpp`	Enters voice MLPP configuration mode.
Step 4	**access-digit** *digit* **Example:** `Router(config-voice-mlpp)# access-digit 8`	Defines the access digit that phone users dial to make an MLPP call. • *digit*—Single-digit number that users dial. Range: 0 to 9. Default: 0. **Note** Your domain type must support the access digit that you select. For example, the valid range for the DSN is 2 to 9.
Step 5	**bnea** *audio-url* **Example:** `Router(config-voice-mlpp)# bnea flash:bnea.au`	Specifies the audio file to play for the busy station not equipped for preemption announcement. • *audio-url*—Location of the announcement audio file in URL format. Valid storage locations are TFTP, FTP, HTTP, and flash memory.
Step 6	**bpa** *audio-url* **Example:** `Router(config-voice-mlpp)# bpa flash:bpa.au`	Specifies the audio file to play for the blocked precedence announcement.

	Command or Action	Purpose
Step 7	**upa** *audio-url* **Example:** `Router(config-voice-mlpp)# upa flash:upa.au`	Specifies the audio file to play for the unauthorized precedence announcement. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 8	**service-domain** { **drsn** | **dsn**}**identifier** *domain-number* **Example:** `Router(config-voice-mlpp)# service-domain dsn 0010`	(Optional) Sets the global MLPP domain type and number. • **drsn**—Defense Red Switched Network (DRSN). • **dsn**—Defense Switched Network (DSN). This is the default value. • *domain-number*—Number to identify the global domain, in three-octet format. Range: 0x000000 to 0xFFFFFF. Default: 0. • A phone uses this global domain for MLPP calls if it is not configured with the **mlpp service-domain** command. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 9	**end** **Example:** `Router(config-voice-mlpp)# end`	Exits to privileged EXEC mode.

Example

The following example shows MLPP enabled on the Cisco Unified CME router.

```
voice mlpp
   access-digit 8
   bpa flash:bpa.au
   bnea flash:bnea.au
   upa flash:upa.au
   service-domain dsn identifier 000010
```

Enable MLPP Service on SCCP Phones

Restriction The **mlpp max-precedence** command is not supported in Cisco Unified CME 8.0 and later versions; it is replaced by the **mlpp service-domain** command.

Before You Begin

MLPP must be enabled globally on the Cisco Unified CME router. See Enable MLPP Service Globally in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **mlpp service-domain**{**drsn** | **dsn**} **identifier** *domain-number* **max-precedence** *level*
5. **mlpp preemption**
6. **mlpp indication**
7. **exit**
8. **ephone** *phone-tag*
9. **ephone-template** *template-tag*
10. **restart**
11. **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-template** *template-tag* **Example:** `Router(config)# ephone-template 15`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 20.
Step 4	**mlpp service-domain**{**drsn** | **dsn**} **identifier** *domain-number* **max-precedence** *level* **Example:** `Router(config-ephone-template)# mlpp service-domain dsn identifier 0010 max-precedence 0`	Sets the service domain and maximum precedence (priority) level for MLPP calls from this phone. • **drsn**—Phone belongs to the Defense Red Switched Network (DRSN). • **dsn**—Phone belongs to the Defense Switched Network (DSN). This is the default value. • *domain-number*—Number to identify the global domain, in three-octet format. Range: 0x000000 to 0xFFFFFF. • *level*—Maximum precedence level. Phone user can specify a precedence level that is less than or equal to this value. ◦ DSN—Range: 0 to 4, where 0 is the highest priority.

	Command or Action	Purpose
		◦ DRSN—Range: 0 to 5, where 0 is the highest priority. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 5	**mlpp preemption** **Example:** `Router(config-ephone-template)# no mlpp preemption`	(Optional) Enables calls on the phone to be preempted. • Preemption is enabled by default. Skip this step unless you want to disable preemption with the **no mlpp preemption** command.
Step 6	**mlpp indication** **Example:** `Router(config-ephone-template)# no mlpp indication`	(Optional) Enables the phone to play precedence and preemption tones, and display the preemption level of calls. • MLPP indication is enabled by default. Skip this step unless you want to disable MLPP indication with the **no mlpp indication** command.
Step 7	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 8	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 9	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 15`	Applies an ephone template to the ephone that is being configured.
Step 10	**restart** **Example:** `Router(config-ephone)# restart`	Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information. **Note** Restart all ephones using the **restart all** command in telephony-service configuration mode.
Step 11	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

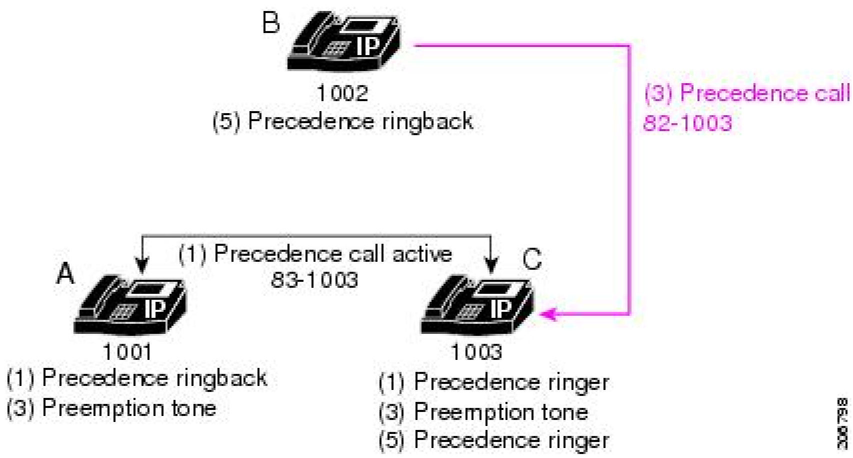
Examples

The following example shows a basic configuration for three phones, all using template 1 with MLPP defined. Figure 34: Preemption Call Example shows an example of a precedence call using this configuration.

```
voice mlpp
   access-digit 8
   bpa flash:BPA.au
   bnea flash:BNEA.au
   upa flash:UPA.au

  ephone-template  1
   mlpp service-domain dsn identifier 000000 max-precedence 0
  !Configures MLPP domain as DSN, identifier as 000000, and max-precedence set to 0

  ephone-dn  1
   number  1001

  ephone-dn  2
   number 1002

  ephone-dn 3 dual-line
   number 1003
   huntstop channel

  ephone 1
   description Phone-A
   mac-address 1111.2222.0001
   button 1:1
   ephone-template 1
  ! MLPP configuration inherited from ephone-template 1

  ephone 2
   description Phone-B
   mac-address 1111.2222.0002
   button 1:2
   ephone-template 1

  ephone-3
   description Phone-C
   mac-address 1111.2222.0003
   button 1:3
   ephone-template 1
```

Note The **huntstop channel** command must be configured on dual-line and octo-line directory numbers to preempt a call on those types of lines. Otherwise the dual-line or octo-line receives Call Waiting indication and the call is not preempted.

Figure 34: Preemption Call Example



In this example, the following sequence of events occurs:

1. Phone A places a precedence call to Phone C by dialing 831003 (access digit 8 + precedence level 3 + destination number 1003).

   Phone C answers the call.

2. Phone C hears the precedence ringer tone and Phone A hears the precedence ringback.
3. Phone B places a higher precedence call to Phone C by dialing 821003. Phone A and Phone C both hear the preemption tone for the duration of the **preemption tone timer** command (default value is three seconds).
4. Phone A is preempted after three seconds.
5. Phone C starts ringing (precedence ringer) and Phone B hears the precedence ringback.
6. Phone C answers the call.

Enable MLPP Service on Analog FXS Phone Ports

Before You Begin

MLPP must be enabled globally on the Cisco Unified CME router. See Enable MLPP Service Globally in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port*
4. **mlpp service-domain**{**drsn** | **dsn**} **identifier** *domain-number* **max-precedence** *level*
5. **mlpp preemption**
6. **mlpp indication**
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-port** *port* **Example:** `Router(config)# voice-port 0/1/0`	Enters voice-port configuration mode. • *Port* argument is platform-dependent; type **?** to display syntax.
Step 4	**mlpp service-domain**{**drsn** | **dsn**} **identifier** *domain-number* **max-precedence** *level* **Example:** `Router(config-voiceport)# mlpp service-domain dsn identifier 0020 max-precedence 0`	Sets the service domain and maximum precedence (priority) level for MLPP calls from this port. • **drsn**—Port belongs to the Defense Red Switched Network (DRSN). • **dsn**—Port belongs to the Defense Switched Network (DSN). • *domain-number*—Number to identify the global domain, in three-octet format. Range: 0x000000 to 0xFFFFFF. • *level*—Maximum precedence level. Phone user can specify a precedence level that is less than or equal to this value. ◦ DSN—Range: 0 to 4, where 0 is the highest priority. ◦ DRSN—Range: 0 to 5, where 0 is the highest priority. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 5	**mlpp preemption**	(Optional) Enables calls on the port to be preempted.

	Command or Action	Purpose
	Example: `Router(config-voiceport)# no mlpp preemption`	• Preemption is enabled by default. Skip this step unless you want to disable preemption with the **no mlpp preemption** command.
Step 6	**mlpp indication** **Example:** `Router(config-voiceport)# no mlpp indication`	(Optional) Enables the phone to play precedence and preemption tones, and display the preemption level of calls. • MLPP indication is enabled by default. Skip this step unless you want to disable MLPP indication with the **no mlpp indication** command.
Step 7	**end** **Example:** `Router(config-voiceport)# end`	Returns to privileged EXEC mode.

Example

The following example shows that the analog FXS phone connected to voice port 0/1/0 can make MLPP calls with the highest precedence and its calls cannot be preempted.

```
voice-port 0/1/0
   mlpp service-domain dsn identifier 000020 max-precedence 0
   no mlpp preemption
   station-id name uut1-fxs1
   caller-id enable
```

Configure an MLPP Service Domain for Outbound Dial Peers

To assign a service domain to MLPP calls that must leave the Cisco Unified CME router through the trunk, perform the following steps for the corresponding dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class mlpp** *tag*
4. **service-domain** {**drsn** | **dsn**}
5. **exit**
6. **dial-peer voice tag** {**pots** | **voip**}
7. **voice-class mlpp** *tag*
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 class mlpp** *tag* **Example:** `Router(config)# voice class mlpp 1`	Creates a voice class for the MLPP service. • *tag*—Unique number to identify the voice class. Range: 1 to 10000.
Step 4	**service-domain** {**drsn** | **dsn**} **Example:** `Router(config-voice-class)# service-domain dsn`	Sets the network domain in the MLPP voice class. • **drsn**—Defense Red Switched Network (DRSN). • **dsn**—Defense Switched Network (DSN).
Step 5	**exit** **Example:** `Router(config-voice-class)# exit`	Exits voice-class configuration mode.
Step 6	**dial-peer voice tag** {**pots** | **voip**} **Example:** `Router(config)# dial-peer voice 101 voip`	Enters dial peer voice configuration mode.
Step 7	**voice-class mlpp** *tag* **Example:** `Router(config-dial-peer)# voice-class mlpp 1`	Assigns a previously configured MLPP voice class to a POTS or VoIP dial peer. • *tag*—Unique number of the voice class that you created in Step 3.
Step 8	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial-peer voice configuration mode.

Example

The following example shows an MLPP voice class defined for the DSN service domain. This voice class is assigned to a POTS dial peer so that calls leaving port 0/1/0 use the DSN protocol.

```
voice class mlpp 1
   service-domain dsn
  !
  !
  dial-peer voice 1011 pots
   destination-pattern 19101
   voice-class mlpp 1
   port 0/1/0
```

Configure MLPP Options

To configure optional MLPP features or modify default settings, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice mlpp**
4. **preemption trunkgroup**
5. **preemption user**
6. **preemption tone timer** *seconds*
7. **preemption reserve timer** *seconds*
8. **service-domain midcall-mismatch**{**method1** | **method2** | **method3** | **method4**}
9. **service-digit**
10. **route-code**
11. **attendant-console** *number* **redirect-timer** *seconds*
12. **ica** *audio-url*
13. **loc2** *audio-url*
14. **vca** *audio-url* **voice-class cause-code** *tag*
15. **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.

	Command or Action	Purpose
Step 3	**voice mlpp** **Example:** `Router(config)# voice mlpp`	Enters voice MLPP configuration mode.
Step 4	**preemption trunkgroup** **Example:** `Router(config-voice-mlpp)# preemption trunkgroup`	Enables preemption capabilities on a trunk group.
Step 5	**preemption user** **Example:** `Router(config-voice-mlpp)# preemption user`	Enables all supported phones to preempt calls.
Step 6	**preemption tone timer** *seconds* **Example:** `Router(config-voice-mlpp)# preemption tone timer 15`	Sets the amount of time that the preemption tone plays on the called phone when a lower precedence call is being preempted. • *seconds*—Expiry time, in seconds. Range: 3 to 30. Default: 0 (disabled).
Step 7	**preemption reserve timer** *seconds* **Example:** `Router(config-voice-mlpp)# preemption reserve timer 10`	Sets the amount of time to reserve a channel for a preemption call. • *seconds*—Range: 3 to 30. Default: 0 (disabled).
Step 8	**service-domain midcall-mismatch**{**method1** | **method2** | **method3** | **method4**} **Example:** `Router(config-voice-mlpp)# service-domain midcall-mismatch method2`	Defines the behavior when there is a domain mismatch between the two legs of a call. • **method1**—Domain remains unchanged for each of the connections and the precedence level of the lower priority call changes to that of the higher priority call. This is the default value. • **method2**—Domain and precedence level of the lower priority call changes to that of the higher priority call. • **method3**—Domain remains unchanged for each of the connections and the precedence levels change to Routine for both calls. • **method4**—Domains change to that of the connection for which supplementary service was invoked (for example, transferee in case of transfer). Precedence levels change to Routine for both calls. • This command is supported in Cisco Unified CME 8.0 and later versions.

	Command or Action	Purpose
Step 9	**service-digit** **Example:** `Router(config-voice-mlpp)# service-digit`	Enables phone users to request off-net services by dialing a service digit. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 10	**route-code** **Example:** `Router(config-voice-mlpp)# route-code`	Enables phone users to specify special routing for a call by dialing a route code. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 11	**attendant-console** *number* **redirect-timer** *seconds* **Example:** `Router(config-voice-mlpp)# attendant-console 8100 redirect-timer 10`	Specifies the telephone number of the MLPP attendant-console service where calls are redirected if the phone does not answer. • *number*—Extension or E.164 telephone number of the Cisco Unified CME basic automatic call distribution (B-ACD) and auto-attendant (AA) service. • *seconds*—Number of seconds to wait for the phone to answer before redirecting the call.
Step 12	**ica** *audio-url* **Example:** `Router(config-voice-mlpp)# ica flash:ica.au`	(Optional) Specifies the audio file to play for the isolated code announcement. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 13	**loc2** *audio-url* **Example:** `Router(config-voice-mlpp)# loc2 flash:loc2.au`	(Optional) Specifies the audio file to play for the loss of C2 features announcement. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 14	**vca** *audio-url* **voice-class cause-code** *tag* **Example:** `Router(config-voice-mlpp)# vca flash:vca.au voice-class cause-code 29`	(Optional) Specifies the audio file to play for the vacant code announcement. • *tag*—Number of the voice class that defines the cause codes for which the VCA is played. Range: 1 to 64. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 15	**end** **Example:** `Router(config-voice-mlpp)# end`	Exits to privileged EXEC mode.

Examples

The following example shows an MLPP configuration with optional parameters.

```
voice mlpp
   preemption trunkgroup
   preemption user
   preemption tone timer 15
   preemption reserve timer 10
   access-digit 8
   attendant-console 8100 redirect-timer 10
   service-digit
   route-code
   bpa flash:bpa.au
   bnea flash:bnea.au
   upa flash:upa.au
   ica flash:ica.au
   loc2 flash:loc2.au
   vca flash:vca.au voice-class cause-code 29
   service-domain midcall-mismatch method2
   service-domain dsn identifier 000010
```

Troubleshooting MLPP Service

SUMMARY STEPS

1. **enable**
2. **debug ephone mlpp**
3. **debug voice mlpp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ephone mlpp** **Example:** `Router# debug ephone mlpp`	Displays debugging information for MLPP calls to phones in a Cisco Unified CME system.
Step 3	**debug voice mlpp** **Example:** `Router# debug voice mlpp`	Displays debugging information for the MLPP service.

Feature Information for MLPP

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

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

Table 68: Feature Information for MLPP

Feature Name	Cisco Unified CME Version	Feature Information
MLPP Enhancements	8.0	Adds support for the following: • Additional MLPP announcements • Multiple service domains • Route codes and service digits • Interaction with supplementary services, such as Three-Way Conference, Call Pickup, and Cancel Call Waiting on Analog FXS ports
MLPP for Cisco Unified CME	7.1	Allows validated users to place priority calls, and if necessary, to preempt lower-priority calls.

CHAPTER 29

Music on Hold

Prerequisites for Music on Hold

- For Unified CME Release 11.6 and previous releases, phones receiving Music on Hold (MOH) in a system using G.729 require transcoding between G.711 and G.729. From Unified CME Release 11.7 onwards, transcoding is not required if G.729 codec format MOH file is configured on Unfiied CME. For information about transcoding, see Configure Transcoding Resources, on page 479.
- Transcoding for MOH is supported on Cisco 4000 Series Integrated Services Router from Unified CME Release 11.7 onwards.

Restrictions for Music on Hold

- IP phones do not support multicast at 224.x.x.x addresses.
- Cisco Unified CME 3.3 and earlier versions do not support MOH for local Cisco Unified CME phones that are on hold with other Cisco Unified CME phones; these parties hear a periodic repeating tone instead.
- Cisco Unified CME 4.0 and later versions support MOH for internal calls on SCCP Phones only if the **multicast moh** command is used to enable the flow of packets to the subnet on which the phones are located.
- Internal extensions that are connected through a Cisco VG224 Analog Voice Gateway or through a WAN (remote extensions) do not hear MOH on internal calls.

- Multicast MOH is not supported on a phone if the phone is configured with the **mtp** command or the **paging-dn** command with the **unicast** keyword.
- For calls from SCCP to SCCP phones, Unicast MoH is not supported. Multicast MoH is supported if it is enabled. If Multicast MoH is not enabled, Tone on Hold is supported.
- Multicast MOH is not supported on SIP Phones.

Information About Music on Hold

Music on Hold Summary

MOH is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls.

Table 69: Music on Hold (MOH) provides a summary of options for MOH for PSTN and multicast MOH for local IP phones.

Table 69: Music on Hold (MOH)

Audio Source	Description	How to Configure
Flash memory	No external audio input is required.	Configure Music on Hold from an Audio File to Supply Audio Stream
Live feed	The multicast audio stream has minimal delay for local IP phones. The MOH stream for PSTN callers is delayed by a few seconds. If the live feed audio input fails, callers on hold hear silence.	Configure Music on Hold from a Live Feed
Live feed and flash memory	The live feed stream has a few seconds of delay for both PSTN and local IP phone callers. The flash MOH acts as backup for the live-feed MoH. If MOH from a live feed is not found or fails, Unified CME swtiches to playback of MOH from the flash memory.	Configure Music on Hold from an Audio File to Supply Audio Stream and Configure Music on Hold from a Live Feed

Music on Hold

MOH is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls.

For Unified CME Release 11.6 and previous releases, when the phone receiving MOH is part of a system that uses a G.729 codec, transcoding is required between G.711 and G.729. The G.711 MOH must be translated to G.729. Note that because of compression, MOH using G.729 is of significantly lower fidelity than MOH using G.711. From Unified CME Release 11.7 onwards, transcoding is not required if G.711 and G.729 codec format MOH files are configured on Unified CME. For information about transcoding, see Configure Transcoding Resources.

The audio stream that is used for MOH can derive from one of two sources:

- Audio file—A MOH audio stream from an audio file is supplied from a .au or .wav file held in router flash memory. For configuration information, see Configure Music on Hold from an Audio File to Supply Audio Stream.
- Live feed—A MOH audio stream from a live feed is supplied from a standard line-level audio connection that is directly connected to the router through an FXO or “ear and mouth” (E&M) analog voice port. For configuration information, see Configure Music on Hold from a Live Feed.

Music on Hold from a Live Feed

The live-feed feature is typically used to connect to a CD jukebox player. To configure MOH from a live feed, you establish a voice port and dial peer for the call and also create a “dummy” ephone-dn. The ephone-dn must have a phone or extension number assigned to it so that it can make and receive calls, but the number is never assigned to a physical phone. Only one live MOH feed is supported per system.

Using an analog E&M port as the live-feed MOH interface requires the minimum number of external components. You 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 voice interface card (VIC) 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.

If you use an FXO port as the live-feed MOH interface, connect the MOH source to the FXO port using a MOD-SC cable if the MOH source has a different connector than the FXO RJ-11 connector. MOH from a live feed is supported on the VIC2-2FXO, VIC2-4FXO, EM-HDA-3FXS/4FXO, EM-HDA-6FXO, and EM2-HDA-4FXO.

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 a MOH live-feed source is attempted (or reattempted) every 30 seconds until the connection is made by the directory number that has been configured for MOH. If the live-feed source is shut down for any reason, the flash memory source will be automatically activated.

A live-feed MOH connection is established as an automatically connected voice call that is made by the Unified CME MOH system 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 optional **out-call** keyword is used with the **moh** command during configuration.

The Unified CME 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 ephone-dn to deliver an audio stream to the Cisco Unified CME router.

For configuration information, see Configure Music on Hold from a Live Feed.

For configuration example, see Examples.

Multicast MOH

In Cisco CME 3.0 and later versions, you can configure the MOH audio stream as a multicast source. A Cisco Unified CME router that is configured for multicast MOH also transmits the audio stream on the physical IP interfaces of the specified router to permit access to the stream by external devices.

Certain IP phones do not support multicast MOH because they do not support IP multicast. In Cisco Unified CME 4.0 and later versions, you can disable multicast MOH to individual phones that do not support multicast. Callers hear a repeating tone when they are placed on hold.

Music on Hold for SIP Phones

In Cisco Unified CME 4.1 and later versions, the MOH feature is supported when a call is put on hold from a SIP phone and when the user of a SIP phone is put on hold by a SIP, SCCP, or POTS endpoint. The holder (party that pressed the hold key) or holdee (party who is put on hold) can be on the same Cisco Unified CME or a different Cisco Unified CME connected through a SIP trunk. MOH is also supported for call transfers and conferencing, with or without a transcoding device.

Configuring MOH for SIP phones is the same as configuring MOH for SCCP phones. For configuration information, see Configure Music on Hold.

Music On Hold Enhancement

Cisco Unified CME 8.0 and later versions enhance the MOH feature by playing different media streams to PSTN and VoIP callers who are placed on hold. The MOH enhancement allows you to configure up to five additional media streams supplied from multiple media files stored in a router's flash memory and eliminates the need for separate routers for streaming MOH media files.

Cisco Unified CME 8.0 MOH enhancement allows you to create MOH groups and assign ephone extension numbers to these MOH groups to receive different media streams. Callers to the extension numbers configured under the MOH groups can listen to different MOH media streams when they are placed on hold.

You can configure up to five MOH groups. The size of each media source file can range between 64KB to 10MB long on the Cisco Unified CME router for ephones in different departments in a branch. A MOH group is linked to an ephone using the extension number of that ephone. For configuration information, see Configure Music on Hold Groups to Support Different Media Sources.

You can also configure individual directory numbers to select any MOH group as a MOH source on the Cisco Unified CME router. The extension number of a directory associates an ephone to a specific MOH group and callers to these extension numbers can listen to different media streams when placed on hold. For configuration information, see Assign a MOH Group to a Directory Number.

Similarly, callers from internal directory numbers can listen to different media streams when a MOH group is assigned for an internal call. For configuration information, see Assign a MOH Group to all Internal Calls Only to SCCP Phones.

Following precedence rules are applicable when an ephone caller is placed on hold:

- **MOH group** defined for internal calls takes highest precedence.
- **MOH group** defined in ephone-dn takes the second highest precedence.
- **MOH group** defined in ephone-dn-template takes precedence if MOH group is not defined in ephone-dn or internal call.
- Extension numbers defined in a **MOH-group** has the least precedence.
- Phones not associated with any MOH groups default to the MOH parameters defined in the **moh** command under telephony-service configuration mode.

Note If a selected MOH group does not exist, the caller will hear tone on hold.

Note We recommend that departments in a branch must have mutually exclusive extension numbers and multicast destinations for configuring MOH groups.

Caching MOH Files for Enhanced System Performance

Caching MOH files helps enhance the system performance by reducing the CPU usage. However, caching requires memory buffer to store a large MOH file. You can set up a buffer file size for caching MOH files that you might use in the future. The default MOH file buffer size is 64 KB (8 seconds). The maximum buffer size (per file) can be configured anywhere between 64 KB (8 minutes) to 10000 KB (approximately 20 minutes), You can use the **moh-file-buffer** command to allocate MOH file buffer for future MOH files, see Configure Buffer Size for MOH Files. To verify if a file is being cached and to update a cached moh-file, see Verify MOH File Caching.

Note If the file size is too large, buffer size falls back to 64 KB.

Configure G.711 and G.729 Files for Music on Hold

From Cisco Unified CME 11.7 Release onwards, G.711 and G.729 codec format MOH files can be configured on Unified CME. For calls (line or trunk calls) that need to be placed on hold and MOH needs to be played, transcode insertion is not required if the codec used is G.729 or G.711. The new feature dynamically selects the matching codec (either G.729 or G.711) based on the codec used on phones or trunk. Transcode insertion is required only if the codec on the phone playing Music on Hold is neither G.729 nor G.711. For more information on configuration of MOH, see Configure Music on Hold, on page 834.

If G.711 and G.729 codec format MOH files are configured on Unified CME, you will need transcoding only to support other codec format MOH files, such as iLBC. You need the G.711 codec format MOH file to be configured under telephony-service for MOH to be supported on Unified CME.

Note You have to configure the primary G.711 codec format MOH file before configuring the G.729 or G.729A codec format MOH file.

We recommend that G.711 and G.729 codec format MOH files are available on the flash memory of Unified CME router.

Note In a scenario where a call between an SCCP line and SIP trunk has a codec other than G.729 or G.711, then MOH is not played when the SCCP line places the SIP phone on hold.

In a scenario where a call is placed between an SCCP line and a SIP line, and the call is placed on hold from the SIP end, MOH is played only from the G.711 codec format MOH file.

Configure Music on Hold

Configure Music on Hold from an Audio File to Supply Audio Stream

Note If you configure MOH from an audio file and from a live feed, the router seeks the live feed first. If a live feed is found, it displaces an audio file source. If the live feed is not found or fails at any time, the router falls back to the audio file source.

Note The MOH file packaged with the CME software is completely royalty free.

Restriction

- To change the audio file to a different file, you must remove the first file using the **no moh** command before specifying a second file. If you configure a second file without removing the first file, the MOH mechanism stops working and may require a router reboot to clear the problem.
- The volume level of a MOH file cannot be adjusted through Cisco IOS software, so it cannot be changed when the file is loaded into the flash memory of the router. To adjust the volume level of a MOH file, edit the file in an audio editor before downloading the file to router flash memory.

Before You Begin

- SIP phones require Cisco Unified CME 4.1 or a later version.
- A music file must be in stored in the router’s flash memory. This file should be in G.711 format. The file can be in .au or .wav file format, but the file format must contain 8-bit 8-kHz data; for example, ITU-T A-law or mu-law data format.
- From Cisco Unified CME Release 11.7 onwards, you can configure and store an MOH file in G.729 codec format in the router's flash memory. The G.729 file can be used as MOH source.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **moh** *filename*
5. **multicast moh** *ip-address* **port** *port-number* [**route** *ip-address-list*]
6. **exit**
7. **ephone** *phone-tag*
8. **multicast-moh**
9. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**moh** *filename* **Example:** `Router(config-telephony)# moh minuet.au`	Enables music on hold using the specified file. • If you specify a file with this command and later want to use a different file, you must disable use of the first file with the **no moh** command before configuring the second file.

	Command or Action	Purpose

	OR
	`Router(config-telephony)# moh flash:moh_g711u_music.wav`
	`Router(config-telephony)# moh g729 flash:SampleAudioSource.g729.wav`
		• G.729 MOH file can be configured along with the G.711 MOH file. Unified CME would pick the MOH file to be played based on the negotiated codec on line or trunk.

Step 5	**multicast moh** *ip-address* **port** *port-number* [**route** *ip-address-list*] **Example:** `Router(config-telephony)# multicast moh 239.10.16.4 port 16384 route 10.10.29.17 10.10.29.33`	Specifies that this audio stream is to be used for multicast and also for MOH. **Note** This command is required to use MOH for internal calls and it must be configured after MOH is enabled with the **moh** command. • *ip-address*—Destination IP address for multicast. • **port** *port-number*—Media port for multicast. Range is 2000 to 65535. We recommend port 2000 because it is already used for normal RTP media transmissions between IP phones and the router. **Note** Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.) • **route**—(Optional) List of explicit router interfaces for the IP multicast packets. • *ip-address-list*—(Optional) List of up to four explicit routes for multicast MOH. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the **ip source-address** command. **Note** For MOH on internal calls, packet flow must be enabled to the subnet on which the phones are located.
Step 6	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 7	**ephone** *phone-tag* **Example:** `Router(config)# ephone 28`	Enters ephone configuration mode.
Step 8	**multicast-moh** **Example:** `Router(config-ephone)# no multicast-moh`	(Optional) Enables multicast MOH on a phone. This is the default. • This command is supported in Cisco Unified CME 4.0 and later versions. • The **no** form of this command disables MOH for phones that do not support multicast. Callers hear a repeating tone when they are placed on hold. • This command can also be configured in ephone-template configuration mode. The value set in ephone configuration mode has priority over the value set in ephone-template mode.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Examples

The following example enables music on hold and specifies the music file to use:

```
telephony-service
   moh minuet.wav
```

The following example enables MOH and specifies a multicast address for the audio stream:

```
telephony-service
   moh minuet.wav
   multicast moh 239.23.4.10 port 2000
```

Configure Music on Hold from a Live Feed

To configure music on hold from a live feed, perform the following steps.

Note If you configure MOH from an audio file and from a live feed, the router seeks the live feed first. If a live feed is found, it displaces an audio file source. If the live feed is not found or fails at any time, the router falls back to the audio file source.

Restriction

- A foreign exchange station (FXS) port cannot be used for a live feed.

Before You Begin

- SIP phones require Cisco Unified CME 4.1 or a later version.
- VIC2-2FXO, VIC2-4FXO, EM-HDA-3FXS/4FXO, EM-HDA-6FXO, or EM2-HDA-4FXO
- For a live feed from VoIP, VAD must be disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port*
4. **input gain** *decibels*
5. **auto-cut-through**
6. **operation 4-wire**
7. **signal immediate**
8. **signal loop-start live-feed**
9. **no shutdown**
10. **exit**
11. **dial peer voice** *tag* **pots**
12. **destination-pattern** *string*
13. **port** *port*
14. **exit**
15. **ephone-dn** *dn-tag*
16. **number** *number*
17. **moh**[**out-call** *outcall-number*] [**ip** *ip-address* **port** *port-number* [**route** *ip-address-list*]]
18. **exit**
19. **ephone** *phone-tag*
20. **multicast-moh**
21. **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-port** *port* **Example:** `Router(config)# voice-port 1/1/0`	Enters voice-port configuration mode. • *Port* argument is platform-dependent; type **?** to display syntax.

	Command or Action	Purpose
Step 4	**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. • *decibels*—Acceptable values are integers –6 to 14.
Step 5	**auto-cut-through** **Example:** `Router(config-voice-port)# 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 6	**operation 4-wire** **Example:** `Router(config-voice-port)# 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 7	**signal immediate** **Example:** `Router(config-voice-port)# 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 dual tone multifrequency (DTMF) digits.
Step 8	**signal loop-start live-feed** **Example:** `Router(config-voice-port)# signal loop-start live-feed`	(FXO ports only) Enables an MOH audio stream from a live feed to be directly connected to the router through an FXO port. • This command is supported in Cisco IOS Release 12.4(15)T and later releases.
Step 9	**no shutdown** **Example:** `Router(config-voice-port)# no shutdown`	Activates the voice port. • To shut the voice port down and disable MOH from a live feed, use the **shutdown** command.
Step 10	**exit** **Example:** `Router(config-voice-port)# exit`	Exits voice-port configuration mode.
Step 11	**dial peer voice** *tag* **pots** **Example:** `Router(config)# dial peer voice 7777 pots`	Enters dial-peer configuration mode.
Step 12	**destination-pattern** *string* **Example:** `Router(config-dial-peer)# destination-pattern 7777`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.

	Command or Action	Purpose
Step 13	**port** *port* **Example:** `Router(config-dial-peer)# port 1/1/0`	Associates the dial peer with the voice port that was specified in Step 3.
Step 14	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.
Step 15	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 55`	Enters ephone-dn configuration mode. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. Range is 1 to 288.
Step 16	**number** *number* **Example:** `Router(config-ephone-dn)# number 5555`	Configures a valid extension number for this ephone-dn. • This number is not assigned to any phone; it is only used to make and receive calls that contain an audio stream to be used for MOH. • *number*—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn.

Step 17	**moh**[**out-call** *outcall-number*] [**ip** *ip-address* **port** *port-number* [**route** *ip-address-list*]]
	
	Example:
	`Router(config-ephone-dn)# moh out-call 7777 ip 239.10.16.8 port 2311 route 10.10.29.3 10.10.29.45`
	or
	`Router(config-ephone-dn)# moh out-call 7777`
		Specifies that this ephone-dn is to be used for an incoming or outgoing call that is the source for an MOH stream.
		• (Optional) **out-call** *outcall-number*—Indicates that the router is calling out for a live feed for MOH and specifies the number to be called. Forces a connection to the local voice port that was specified in Step 3. If this command is used without this keyword, the MOH stream is received from an incoming call.
		• (Optional) **ip** *ip-address*—Destination IP address for multicast.
		If you are configuring MOH from a live feed and from an audio file for backup, do not configure a multicast IP address for this command. If the live feed fails or is not found, MOH will fall back to the ip address that you configured using the **multicast moh** command in telephony-service configuration mode. See Configure Music on Hold from an Audio File to Supply Audio Stream.
		If you specify an address for multicast with this command and a different address with the **multicast moh** command in telephony-service configuration mode, you can send the MOH audio stream to two multicast addresses.
		• (Optional) **port** *port-number*—Media port for multicast. Range is 2000 to 65535. We recommend port 2000 because it is already used for RTP media transmissions between IP phones and the router.
		• (Optional) **route** *ip-address*-list—Indicates specific router interfaces on which to transmit the IP multicast packets. Up to four IP addresses

	Command or Action	Purpose
		can be listed. Default: The MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the **ip source-address** command.
Step 18	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 19	**ephone** *phone-tag* **Example:** `Router(config)# ephone 28`	Enters ephone configuration mode.
Step 20	**multicast-moh** **Example:** `Router(config-ephone)# no multicast-moh`	(Optional) Enables multicast MOH on a phone. This is the default. • This command is supported in Cisco Unified CME 4.0 and later versions. • The **no** form of this command disables MOH for phones that do not support multicast. Callers hear a repeating tone when they are placed on hold. • This command can also be configured in ephone-template configuration mode. The value set in ephone configuration mode has priority over the value set in ephone-template mode.
Step 21	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Examples

The following example enables MOH from an outgoing call on voice port 1/1/0 and dial peer 7777:

```
voice-port 1/1/0
 auto-cut-through
 operation 4-wire
 signal immediate
!
dial-peer voice 7777 pots
 destination-pattern 7777
 port 1/1/0
!
ephone-dn 55
 number 5555
 moh out-call 7777
```

The following example enables MOH from a live feed and if the live feed is not found or fails at any time, the router falls back to the music file (music-on-hold.au) and multicast address for the audio stream specified in the telephony-service configuration:

```
voice-port 0/1/0
 auto-cut-through
 operation 4-wire
 signal immediate
 timeouts call-disconnect 1
 description MOH Live Feed
!
dial-peer voice 7777 pots
 destination-pattern 7777
 port 0/1/0
!
telephony-service
 max-ephones 24
 max-dn 192
 ip source-address 10.232.222.30 port 2000
 moh music-on-hold.au
 multicast moh 239.1.1.1 port 2000
!
ephone-dn  52
   number 1
 moh out-call 7777
```

Configure Music on Hold Groups to Support Different Media Sources

Restriction

- Media files from live-feed source are not supported.
- Each MOH group must contain a unique flash media file name, extension numbers, and multicast destination. If you enter any extension ranges, MOH filenames, and multicast IP addresses that already exist in another MOH-group, an error message is issued and the new input in the current voice MOH-group is discarded.
- Media file CODEC format is limited to G.711 and G.729.

Before You Begin

- Cisco Unified CME 8.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice moh-group** *moh-group-tag*
4. **description** *string*
5. **moh** *filename*
6. **multicast moh** *ip-address* **port** *port-number* **route** *ip-address-list*
7. **extension-range** *starting-extension to ending-extension*
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 moh-group** *moh-group-tag* **Example:** `Router(config-telephony)# voice moh-group 1`	Enters the voice moh-group configuration mode. You can create up to five voice moh-groups for ephones receiving music on hold audio files when placed on hold. Range for the voice moh-groups is 1 to 5.
Step 4	**description** *string* **Example:** `Router(config-voice-moh-group)# description moh group for sales`	(Optional) Allows you to add a brief description specific to a voice MOH group. You can use up to 80 characters to describe the voice MOH group.
Step 5	**moh** *filename* **Example:** `Router(config-voice-moh-group)# moh flash:/minuet.au`	Enables music on hold using the specified MOH source file. The MOH file must be in .au and .wav format. MOH filename length should not exceed 128 characters. You must provide the directory and filename of the MOH file in URL format. For example: **moh flash:/minuet.au** • If you specify a file with this command and later want to use a different file, you must disable use of the first file with the **no moh** command before configuring the second file.
Step 6	**multicast moh** *ip-address* **port** *port-number* **route** *ip-address-list* **Example:** `Router((config-voice-moh-group)# multicast moh 239.10.16.4 port 16384 route 10.10.29.17 10.10.29.33`	Specifies that this audio stream is to be used for multicast and also for MOH. **Note** This command is required to use MOH for internal calls and it must be configured after MOH is enabled with the **moh** command. • *ip-address*—Destination IP address for multicast. • **port** *port-number*—Media port for multicast. Range is 2000 to 65535. We recommend port 2000 because it is already used for normal RTP media transmissions between IP phones and the router. **Note** Valid port numbers for multicast include even numbers that range from 16384 to 32767. (The system reserves odd values.)

	Command or Action	Purpose
		• **route**—(Optional) List of explicit router interfaces for the IP multicast packets. • *ip-address-list*—(Optional) List of up to four explicit routes for multicast MOH. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the **ip source-address** command. **Note** For MOH on internal calls, packet flow must be enabled to the subnet on which the phones are located.

Step 7	**extension-range** *starting-extension to ending-extension*
	Example:
	`Router(config-voice-moh-group)#extension-range 1000 to 1999`
	`Router(config-voice-moh-group)#extension-range 2000 to 2999`
		(Optional) identifies MOH callers calling the extension numbers specified in a MOH group. Extension number must be in hexadecimal digits (0-9) or (A-F). Both extension numbers (starting extension and ending extension) must contain equal number of digits. Repeat this command to add additional extension ranges.
		• *starting-extension*—(Optional) Lists the starting extension number for a moh-group.
		• *ending-extension*—(Optional) Lists the ending extension number for a moh-group.
		Note The ending extension number must be greater than or equal to the starting extension number. Extension-ranges must not overlap with any other extension-range configured in any other MOH group.
		Note If extension range is defined and a moh-group is also defined in an **ephone-dn**, the **ephone-dn** parameters takes precedence.

Step 8	**end** **Example:** `Router(config-voice-moh-group)# end`	Returns to privileged EXEC mode.

Examples

In the following example, total six MOH groups are configured. MOH group 1 through 5 are configured under voice-moh-group configuration mode and MOH group 0 is the MOH source file configured under telephony-services.

```
 router# show voice moh-group
 telephony-service
 moh alaska.wav
 Moh multicast 239.1.1.1 port 16384 route 10.1.4.31 10.1.1.2

voice moh-group 1
 description this moh group is for sales
 moh flash:/hello.au
 multicast moh 239.1.1.1 port 16386 route 239.1.1.3 239.1.1.3
 extension-range 1000 to 1999
```

```
 extension-range 2000 to 2999
 extension-range 3000 to 3999
 extension-range A1000 to A1999

voice moh-group 2
 description (not configured)
 moh flash1:/minuet.au
 multicast moh 239.23.4.10 port 2000
 extension-range 7000 to 7999
 extension-range 8000 to 8999

voice moh-group 3
 description This is for marketing
 moh flash2:/happy.au
 multicast moh 239.15.10.1 port 3000
 extension-range 9000 to 9999

voice moh-group 4
 description (not configured)
 moh flash:/audio/sun.au
 multicast moh 239.16.12.1 port 4000
 extension-range 10000 to 19999

voice moh-group 5
 description (not configured)
 moh flash:/flower.wav
 multicast moh 239.12.1.2 port 5000
 extension-range 0012 to 0024
 extension-range 0934 to 0964

=== Total of 6 voice moh-groups ===
```

Assign a MOH Group to a Directory Number

Restriction

- Do not use same extension number for different MOH groups.

Before You Begin

- Cisco Unified CME 8.0 or a later version.
- MOH groups must be configured under global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** tag
4. **number**
5. **moh-group** *tag*
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	**ephone-dn** tag **Example:** `Router(config)# ephone-dn 1`	Enters **ephone-dn** configuration mode. In ephone-dn configuration mode, you assign an extension number using the number command. You can also configure a MOH group to an ephone-dn- template for use across a range of ephone-dns. If two different MOH groups are configured as a result of this command, the MOH group configured under the ephone-dn configuration takes precedence. **Note** MOH group configuration for ephone-template-dn configuration command is temporarily prohibited when any directory number using that template is on hold.

Step 4	**number**
	
	Example:
	`Router(config)# ephone-dn 1`
	`Router(config-ephone-dn)# number 1001`
		Allows you to define an extension number and associate this number to a telephone.

Step 5	**moh-group** *tag*
	
	Example:
	`Router(config-telephony)#voice moh-group 1`
	`Router(config-voice-moh-group)#`
		Allows you to assign a MOH group to a directory number.
		• MOH group *tag*— identifies the unique number assigned to a MOH group for configuration tasks.

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

Examples

In the following example different moh groups are assigned to different directory numbers (ephone-dn) moh group1 is assigned to ephone-dn 1, moh-group 4 is assigned to ephone-dn 4, and moh-group 5 is assigned to ephone-dn 5.

```
ephone-dn  1  octo-line
 number 7001
 name DN7001
 moh-group 1
!
ephone-dn  2  dual-line
 number 7002
 name DN7002
 call-forward noan 6001 timeout 4
!
ephone-dn  3
 number 7003
 name DN7003
 snr 7005 delay 3 timeout 10
 allow watch
 call-forward noan 8000 timeout 30
!
!
ephone-dn  4  dual-line
 number 7004
 allow watch
 call-forward noan 7001 timeout 10
 moh-group 4
 !
ephone-dn  5
 number 7005
 name DN7005
 moh-group 5
 !
```

Assign a MOH Group to all Internal Calls Only to SCCP Phones

Restriction

- Do not use same extension number for different MOH groups.

Before You Begin

- Cisco Unified CME 8.0 or a later version.
- MOH groups must be configured under global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **internal-call moh-group** *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	**telephony-service** **Example:** `Router(config-telephony)# ephone-dn 1`	Enters telephony-service configuration mode. In ephone-dn configuration mode, you assign an extension number using the number command.

Step 4	**internal-call moh-group** *tag*
	
	Example:
	`Router(config)#`
	
	`Router(config-telephony)# internal call moh-group 4`
		Allows to assign a MOH-group for all internal directory numbers.
		• Moh group *tag*— identifies the unique number assigned to a MOH group for configuration tasks, Range for the tag is from 0 to 5, where 0 represents MOH configuration in telephony service.

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

Examples

The following examples shows moh-group 4 configured for internal directory calls.

```
telephony-service
  sdspfarm conference mute-on *6 mute-off *8
  sdspfarm units 4
  sdspfarm transcode sessions 2
  sdspfarm tag 1 moto-HW-Conf
  moh flash1:/minuet.au
  Moh multicast 239.1.1.1 port 16384 route 10.1.4.31 10.1.1.2
  internal-call moh-group 4
  em logout 0:0 0:0 0:0
  max-ephones 110
  max-dn 288
  ip source-address 15.2.0.5 port 2000
  auto assign 1 to 1
  caller-id block code *9999
  service phone settingsAccess 1
  service phone spanTOPCPort 0
  service dss
  timeouts transfer-recall 12
```

Configure Buffer Size for MOH Files

Restriction

- MOH file caching is prohibited if live-feed is enabled for MOH-group 0.
- MOH file buffer size must be larger than the MOH file (size) that needs to be cached.
- Sufficient system memory must be available for MOH file caching.

Before You Begin

- Cisco Unified CME 8.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **moh-file-buffer** *file size*
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	**telephony-service** **Example:** `Router(config-telephony)# ephone-dn 1`	Enters telephony-service configuration mode. In ephone-dn configuration mode, you assign an extension number using the number command.
Step 4	**moh-file-buffer** *file size* **Example:** `Router(config-telephony)# moh-file-buffer 2000`	(Optional) Allows to set a buffer for the MOH file size. You can configure a max file buffer size (per file) anywhere between 64 KB (8 seconds) to 10000 KB (approximately 20 minutes), Default **moh-file-buffer** size is 64 KB (8 seconds). **Note** A large buffer size is desirable to cache the largest MOH file and a better system performance.

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

Examples

The following examples shows 90 KB as the configured moh-file-buffer size.

```
telephony-service
 sdspfarm conference mute-on *6 mute-off *8
 sdspfarm units 4
 sdspfarm transcode sessions 2
 sdspfarm tag 1 moto-HW-Conf
 moh flash1:/minuet.au
 Moh multicast 239.1.1.1 port 16384 route 10.1.4.31 10.1.1.2
 moh-file-buffer 90
 em logout 0:0 0:0 0:0
 max-ephones 110
 max-dn 288
 ip source-address 15.2.0.5 port 2000
 auto assign 1 to 1
 caller-id block code *9999
 service phone settingsAccess 1
 service phone spanTOPCPort 0
 service dss
 timeouts transfer-recall 12
```

Verify MOH File Caching

Use the **show ephone moh** command to verify if the MOH file is being cached.
The following examples shows that the minuet.au music file in MOH group 1 is not cached. Follow steps a through d to verify the MOH file is being cached.

Example:

```
Router #show ephone moh
Skinny Music On Hold Status (moh-group 1)
Active MOH clients 0 (max 830), Media Clients 0
File flash:/minuet.au (not cached) type AU Media_Payload_G711Ulaw64k 160 bytes
Moh multicast 239.10.16.6 port 2000
```

a) If the file is not cached as in MOH group 1 in the above example, then check file size in the flash.

Example:

```
Router#dir flash:/minuet.au
Directory of flash:/minuet.au 32  -rw- 1865696  Apr 25 2009 00:47:12 +00:00  moh1.au
```

b) Under telephony-service, configure “moh-file-buffer <file size>”. Default file size is 64 KB (8 seconds). Make sure you enter a larger file size to cache large MOH files that you may use in future.

Example:

```
Router(config)# telephony-service
Router(config-telephony)# moh-file-buffer 2000
```

c) Under voice moh-group <group tag>, configure “no moh”, and immediately configure “moh <filename>”. This allows the MOH server to read the file immediately from flash again.

Example:

```
Router(config-telephony)#voice moh-group 1
Router(config-voice-moh-group)#no moh
Router(config-voice-moh-group)#moh flash:/minuet.au
```

d) Depending on the size of the file, you should see the MOH file caching after a few minutes (approximately, 2 minutes).

Example:

```
Router #show ephone moh
Skinny Music On Hold Status - group 1
Active MOH clients 0 (max 830), Media Clients 0
File flash:/moh1.au (cached) type AU Media_Payload_G711Ulaw64k 160 bytes
Moh multicast 239.10.16.6 port 2000
```

Note MOH file caching is prohibited under the following conditions: if live feed is configured in moh-group 0, If file buffer size smaller than file size, or insufficient system memory.

Verify Music on Hold Group Configuration

Step 1 Use the **show voice moh-group** command to display one or the entire moh-group configuration.
The following example shows all six MOH groups with extension ranges, MOH files, and multicast destination addresses.

```
router# show voice moh-group
 telephony-service
 moh alaska.wav
 Moh multicast 239.1.1.1 port 16384 route 10.1.4.31 10.1.1.2

voice moh-group 1
 description this moh group is for sales
 moh flash:/audio?minuet.au
 multicast moh 239.1.1.1 port 16386 route 239.1.1.2 239.1.1.3
 extension-range 1000 to 1999
 extension-range 2000 to 2999
 extension-range 3000 to 3999
 extension-range 20000 to 22000
 extension-range A1000 to A1999

voice moh-group 2
```

```
 description (not configured)
 moh flash:/audio/hello.au
 multicast moh 239.23.4.10 port 2000
 extension-range 7000 to 7999
 extension-range 8000 to 8999

voice moh-group 3
 description This is for marketing
 moh flash:/happy.au
 multicast moh 239.15.10.1 port 3000
 extension-range 9000 to 9999

voice moh-group 4
 description (not configured)
 moh flash:/audio/sun.au
 multicast moh 239.16.12.1 port 4000
 extension-range 10000 to 19999

voice moh-group 5
 description (not configured)
 moh flash:/flower.wav
 multicast moh 239.12.1.2 port 5000
 extension-range 0012 to 0024
 extension-range 0934 to 0964

=== Total of 6 voice moh-groups ===
```

Step 2 Use the **show ephone moh** to display information about the different MOH group configured. The following example displays information about five different MOH groups.

```
Router # show ephone moh
Skinny Music On Hold Status (moh-group 1)
Active MOH clients 0 (max 830), Media Clients 0
File flash:/minuet.au (not cached) type AU Media_Payload_G711Ulaw64k 160 bytes
Moh multicast 239.10.16.6 port 2000

Skinny Music On Hold Status (moh-group 2)
Active MOH clients 0 (max 830), Media Clients 0
File flash:/audio/hello.au type AU Media_Payload_G711Ulaw64k  160 bytes
Moh multicast on 239.10.16.6 port 2000 via 0.0.0.0

Skinny Music On Hold Status (moh-group 3)
Active MOH clients 0 (max 830), Media Clients 0
File flash:/bells.au type AU Media_Payload_G711Ulaw64k  160 bytes
Moh multicast on 239.10.16.5 port 2000 via 0.0.0.0

Skinny Music On Hold Status (moh-group 4)
Active MOH clients 0 (max 830), Media Clients 0
File flash:/3003.au type AU Media_Payload_G711Ulaw64k  160 bytes
Moh multicast on 239.10.16.7 port 2000 via 0.0.0.0

Skinny Music On Hold Status (moh-group 5)
```

```
Active MOH clients 0 (max 830), Media Clients 0
File flash:/4004.au type AU Media_Payload_G711Ulaw64k  160 bytes
Moh multicast on 239.10.16.8 port 2000 via 0.0.0.0
```

Step 3 Use the **show voice moh-group statistics** command to display the MOH subsystem statistics information.
In the following example, the MOH Group Streaming Interval Timing Statistics shows the media packet counts during streaming intervals. Each packet counter is of 32 bit size and holds a count limit of 4294967296. This means that with 20 milliseconds packet interval (for G.711), the counters will restart from 0 any time after 2.72 years (2 years 8 months). Use the clear voice moh-group statistics once in every two years to reset the packet counters.

MOH Group Packet Transmission Timing Statistics shows the maximum and minimum amount of time (in microseconds) taken by the MOH groups to send out media packets. The MOH Group Loopback Interval Timing Statistics is available when loopback interface is configured as part of the multicast MOH routes as in the case of SRST. These counts are loopback packet counts within certain streaming timing intervals.

```
router# show voice moh-group statistics

MOH Group Streaming Interval Timing Statistics:
Grp#  ~19 msec     20~39      40~59      60~99     100~199   200+ msec
==== ========== ========== ========== ========== ========== ==========
 0:       25835   17559966      45148          0          0          1
 1:       19766   17572103      39079          0          0          1
 2:       32374   17546886      51687          0          0          1
 3:       27976   17555681      47289          0          0          1
 4:       34346   17542940      53659          0          0          1
 5:       14971   17581689      34284          0          0          1

MOH Group Packet Transmission Timing Statistics:
Grp#  max(usec)  min(usec)
==== ========== ==========
 0:          97          7.
 1:          95          7.
 2:          97          7.
 3:          96          7.
 4:          94          7.
 5:          67          7.

 MOH Group Loopback Interval Timing Statistics:
 loopback event array: svc_index=1542, free_index=1549, max_q_depth=31
 Grp#  ~19 msec     20~39      40~59      60~99     100~199   200+ msec
 ==== ========== ========== ========== ========== ========== ==========
 0:     8918821    8721527      10023          0          1          1
 1:     9007373    8635813       7184          0          1          1
 2:     8864760    8772851      12758          0          1          1
 3:     8924447    8715457      10464          0          1          1
 4:     8858393    8778957      13017          0          1          1
 5:     9005511    8639936       4919          0          1          1

Statistics collect time: 4 days 2 hours 5 minutes 39 seconds.
```

Step 4 Use the **clear voice moh-group statistics** command to clear the display of MOH subsystem statistics information.

For Example:

```
router# clear voice moh-group statistics
All moh group stats are cleared
```

Feature Information for Music on Hold

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

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

Table 70: Feature Information for Music on Hold

Feature Name	Cisco Unified CME Version	Feature Information
Music on Hold	11.7	Support for configuration of G.711 and G.729 codec format MOH file on Unified CME is added.
	8.0	Music on hold from different media sources is added.
	4.1	Music on hold for SIP phones is supported.
	4.0	• Music on hold is introduced for internal calls. • The ability to disable multicast MOH per phone is introduced.
	3.0	The ability to use a live audio feed as a multicast source is introduced.
	2.1	Music on hold from a live audio feed is introduced for external calls.
	2.0	Music on hold from an audio file is introduced for external calls.

CHAPTER 30

Paging

Restrictions for Paging

- Paging is not supported on IP phones without speaker phones.
- Paging is not supported on Cisco Unified 3905 SIP IP phones.
- Paging is only supported on G711ulaw codec.

Information About Paging

Audio Paging

A paging number can be defined to relay audio pages to a group of designated phones. When a caller dials the paging number (ephone-dn), each idle IP phone that has been configured with the paging number automatically answers using its speaker-phone mode. Displays on the phones that answer the page show the caller ID that has been set using the **name** command under the paging ephone-dn. When the caller finishes speaking the message and hangs up, the phones are returned to their idle states.

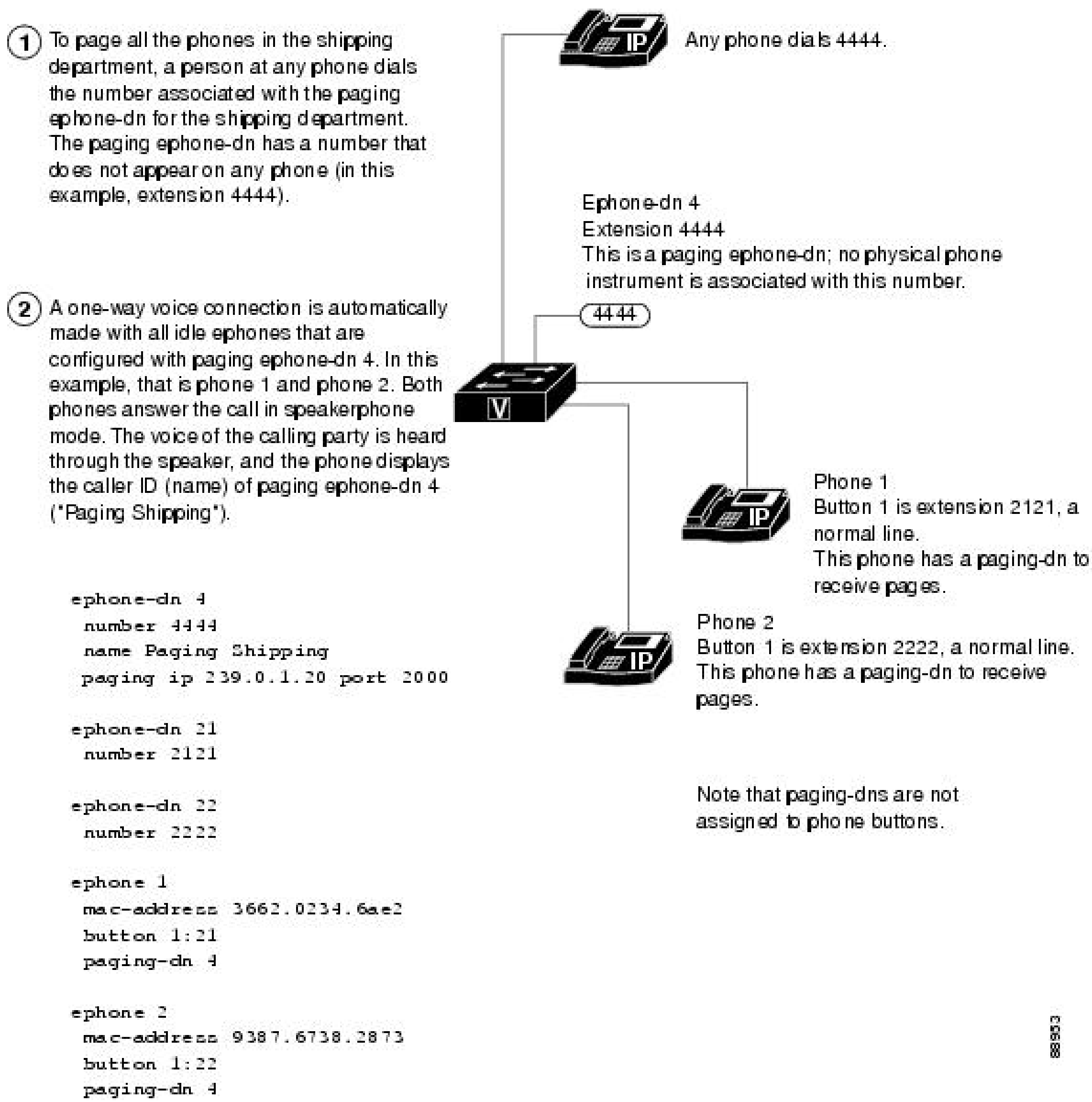
Audio paging provides a one-way voice path to the phones that have been designated to receive paging. It does not have a press-to-answer option like the intercom feature. A paging group is created using a dummy ephone-dn, known as the paging ephone-dn, that can be associated with any number of local IP phones. The paging ephone-dn can be dialed from anywhere, including on-net.

After you have created two or more simple paging groups, you can unite them into combined paging groups. By creating combined paging groups, you provide phone users with the flexibility to page a small local paging group (for example, paging four phones in a store's jewelry department) or to page a combined set of several paging groups (for example, by paging a group that consists of both the jewelry department and the accessories department).

The paging mechanism supports audio distribution using IP multicast, replicated unicast, and a mixture of both (so that multicast is used where possible, and unicast is used for specific phones that cannot be reached using multicast).

Figure 35: Paging Group, on page 858 shows a paging group with two phones.

Figure 35: Paging Group



Paging Group Support for Cisco Unified SIP IP Phones

Paging provides a one-way voice path from the paging phone to the paged phone. The paged phone automatically answers the page in speaker-phone mode with Mute activated.

The paged phone receives a page when it is idle or busy. When it is busy with a connected call, the user of the paged phone can hear both the active conversation and whisper paging.

Before Cisco Unified CME 9.0, you can specify a paging-dn tag and dial the paging extension number to page the Cisco Unified SCCP IP phone associated with the paging-dn tag or paging group using the **paging-dn** command in ephone or ephone-template configuration mode. You can also page a combined paging group composed of two or more previously established paging groups of Cisco Unified SCCP IP phone directory numbers using the **paging group** command in ephone-dn configuration mode.

In Cisco Unified CME 9.0 and later versions, support is extended so that you can specify a paging-dn tag and dial the paging extension number to page the Cisco Unified SIP IP phone associated with the paging-dn tag or paging group using the **paging-dn** command in voice register pool or voice register template configuration mode. Paging on Cisco Unified SIP IP phones support both unicast and multicast paging in the same way that these features are supported on Cisco Unified SCCP IP Phones.

In Cisco Unified CME 9.0 and later versions, support is also extended so that you can create a combined paging group composed of two or more previously established paging groups of ephone and voice register directory numbers using the same **paging group** command used for paging groups of Cisco Unified SCCP IP phone directory numbers.

Note The paging port for Cisco Unified SIP IP phones is an even number from 20480 to 32768. If you enter a wrong port number, a SIP REFER message request is sent to the IP phone but the Cisco Unified SIP IP phone is not paged.

With a paging-dn, there is only one paging endpoint and there is only one paging number for both Cisco Unified SCCP and Cisco Unified SIP IP phones. However, when paging to a Cisco Unified SIP shared line, each phone on the shared line is treated separately.

A phone that can be paged by two paging-dns receives the page from the first paging-dn and ignores the page from the second paging-dn. When the first paging-dn is disconnected, the phone can receive the page from the second paging-dn.

The paging group support for Cisco Unified SIP IP phones uses an ephone paging-dn to dial the paging number before branching out to each Cisco Unified SCCP and Cisco Unified SIP IP phone.

The show **ephone-dn paging** command displays which paging-dn is specified and which phone is being paged.

Because paging is not considered a call, a paging phone that is in a connected state can press another line to make a call using the phone's softkeys.

The Cisco Unified SIP IP phone Paging feature also supports:

- multicast paging (default)
- unicast paging

For more information, see Configure Paging Group Support for SIP IP Phones, on page 864.

Configure Paging

Configure a Simple Paging Group on SCCP Phones

To set up a paging number that relays incoming pages to a group of phones, perform the following steps.

Restriction IP phones do not support multicast at 224.x.x.x addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *paging-dn-tag*
4. **number** *number*
5. **name** *name*
6. **paging** [**ip** *multicast-address* **port** *udp-port-number*]
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	**ephone-dn** *paging-dn-tag* **Example:** `Router(config)# ephone-dn 42`	Enters ephone-dn configuration mode. • *paging-dn-tag*—A unique sequence number that identifies this paging ephone-dn during all configuration tasks. This is the ephone-dn that is dialed to initiate a page. This ephone-dn is not associated with a physical phone. Range is 1 to 288. **Note** Do not use the **dual-line** keyword with this command. Paging ephone-dns cannot be dual-line.

	Command or Action	Purpose
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 3556`	Defines an extension number associated with the paging ephone-dn. This is the number that people call to initiate a page.
Step 5	**name** *name* **Example:** `Router(config-ephone-dn)# name paging4`	Assigns to the paging number a name to appear in caller-ID displays and directories.
Step 6	**paging** [**ip** *multicast-address* **port** *udp-port-number*] **Example:** `Router(config-ephone-dn)# paging ip 239.1.1.10 port 2000`	Specifies that this ephone-dn is to be used to broadcast paging messages to the idle IP phones that are associated with the paging dn-tag. If the optional keywords and arguments are not used, IP phones are paged individually using IP unicast transmission (to a maximum of ten IP phones). The optional keywords and arguments are as follows: • **ip** *multicast-address* **port** *udp-port-number*—Specifies multicast broadcast using the specified IP address and UDP port. When multiple paging numbers are configured, each paging number must use a unique IP multicast address. We recommend port 2000 because it is already used for normal non-multicast RTP media streams between phones and the Cisco Unified CME router. **Note** IP phones do not support multicast at 224.x.x.x addresses. **Note** The correct paging port for the paging-dn of Cisco Unified SIP IP phones is an even number from 20480 to 32768. If you enter a wrong port number, a SIP REFER message request is sent to the IP phone but the Cisco Unified SIP IP phone is not paged.
Step 7	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure a Combined Paging Group for SCCP Phones

To set up a combined paging group consisting of two or more simple paging groups, perform the following steps.

Before You Begin

Simple paging groups must be configured. See Configure a Simple Paging Group on SCCP Phones, on page 860.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *paging-dn-tag*
4. **number** *number*
5. **name** *name*
6. **paging group** *paging-dn-tag*, *paging-dn-tag* [[**,***paging-dn-tag*]**...**]
7. **exit**
8. **ephone** *phone-tag*
9. **paging-dn** *paging-dn-tag* {**multicast** | **unicast**}
10. **exit**
11. Repeat Step 8 to Step 10 to add additional IP phones to a paging group.
12. **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-dn** *paging-dn-tag* **Example:** `Router(config)# ephone-dn 42`	Enters ephone-dn configuration mode to create a paging number for a combined paging group. • *paging-dn-tag*—A unique sequence number that identifies this paging ephone-dn during all configuration tasks. This is the ephone-dn that is dialed to initiate a page. This ephone-dn is not associated with a physical phone. Range is 1 to 288. **Note** Do not use the **dual-line** keyword with this command. Paging ephone-dns cannot be dual-line.
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 3556`	Defines an extension number associated with the combined group paging ephone-dn. This is the number that people call to initiate a page to the combined group.

	Command or Action	Purpose
Step 5	**name** *name* **Example:** `Router(config-ephone-dn)# name paging4`	(Optional) Assigns to the combined group paging number a name to appear in caller-ID displays and directories.
Step 6	**paging group** *paging-dn-tag*, *paging-dn-tag* [[,*paging-dn-tag*]...] **Example:** `Router(config-ephone-dn)# paging group 20,21`	Sets the paging directory number for a combined group. This command combines the individual paging group ephone-dns that you specify into a combined group so that a page can be sent to more than one paging group at a time. • *paging-dn-tag*—Unique sequence number associated with the paging number for an individual paging group. Lists the paging-dn-tags of all the individual groups that you want to include in this combined group, separated by commas. You can include up to ten paging ephone-dn tags in this command. **Note** Configure the paging command for all ephone-dns in a paging group before configuring the paging group command for that group.
Step 7	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 8	**ephone** *phone-tag* **Example:** `Router(config)# ephone 2`	Enters ephone configuration mode to add IP phones to the paging group. • *phone-tag*—Unique sequence number of a phone to receive audio pages when the paging ephone-dn is called.
Step 9	**paging-dn** *paging-dn-tag* {**multicast** | **unicast**} **Example:** `Router(config-ephone)# paging-dn 42 multicast`	Associates this ephone with an ephone-dn tag that is used for a paging ephone-dn (the number that people call to deliver a page). Note that the paging ephone-dn tag is not associated with a line button on this ephone. The paging mechanism supports audio distribution using IP multicast, replicated unicast, and a mixture of both (so that multicast is used where possible and unicast is allowed to specific phones that cannot be reached through multicast). • *paging-dn-tag*—Unique sequence number for a paging ephone-dn. • **multicast**—(Optional) Multicast paging for groups. By default, paging is transmitted to the Cisco Unified IP phone using multicast. • **unicast**—(Optional) Unicast paging for a single Cisco Unified IP phone. This keyword indicates that the Cisco Unified IP phone is not capable of receiving paging through multicast and requests that the phone receive paging through a unicast transmission directed to the individual phone. **Note** The number of phones supported through unicast is limited to a maximum of ten phones.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode.
Step 11	Repeat Step 8 to Step 10 to add additional IP phones to a paging group.	—
Step 12	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Paging Group Support for SIP IP Phones

Note

- Paging Group is supported in Cisco Unified CME but not in Cisco Unified SRST.
- Paging is not supported on Cisco Unified 3905 SIP IP phones.
- Cisco Unified SCCP IP phones do not support whisper paging. Only idle IP phones can receive paging requests.

Before You Begin

Cisco Unified CME 9.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number*
5. **paging** [**ip** *multicast-address* **port** *udp-port-number*]
6. Repeat Step 3 to Step 5 to add more Cisco Unified SCCP IP phones to the paging group. Skip Step 7 for each IP phone except for the last one.
7. **paging group** *paging-dn-tag*, *paging-dn-tag*
8. **exit**
9. **voice register dn** *dn-tag*
10. **number** *number*
11. **exit**
12. Repeat Step 9 to Step 11 to associate more telephone or extension numbers with Cisco Unified SIP IP phones.
13. **voice register pool** *pool-tag*
14. **id mac** *address*
15. **type** *phone-type*
16. **number** *tag* **dn** *dn-tag*
17. **paging-dn** *paging-dn-tag*
18. Repeat Step 13 to Step 17 to register additional Cisco Unified SIP IP phones to ephone-dn paging directory numbers. Exit from voice register pool configuration mode after each additional phone is registered. After the last phone is added, go directly to Step 19.
19. **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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 20`	Enters ephone-dn configuration mode. • *dn-tag*—Unique number that identifies an ephone-dn during configuration tasks. Range is 1 to the number set by the **max-dn** command.

	Command or Action	Purpose
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 2000`	Associates a telephone or extension number with this ephone-dn. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally, the string is composed of digits, but the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number. One or more periods (.) can be used as wildcard characters.
Step 5	**paging** [**ip** *multicast-address* **port** *udp-port-number*] **Example:** `Router(config-ephone-dn)# paging ip 239.0.1.20 port 20480`	Defines an extension (ephone-dn) as a paging extension that can be called to broadcast an audio page to a set of Cisco Unified IP phones. • **ip** *multicast-address*—(Optional) Uses an IP multicast address to multicast voice packets for audio paging; for example, 239.0.1.1. **Note** IP phones do not support multicast at 224.x.x.x addresses. Default is that multicast is not used and IP phones are paged individually using IP unicast transmission (up to ten phones). • **port** *udp-port-number*—(Optional) Uses this UDP port for the multicast. Range: 2000 to 65535. **Note** If any of the paged phones is a Cisco Unified SIP IP phone, the correct paging port for the paging-dn is an even number from 20480 to 32768. If you enter a wrong port number, a SIP REFER message request is sent to the IP phone but the Cisco Unified SIP IP phone is not paged.
Step 6	Repeat Step 3 to Step 5 to add more Cisco Unified SCCP IP phones to the paging group. Skip Step 7 for each IP phone except for the last one.	—
Step 7	**paging group** *paging-dn-tag*, *paging-dn-tag* **Example:** `Router(config-ephone-dn)# paging group 20`	Creates a combined paging group from two or more previously established paging sets. • *paging-dn-tag*—Comma-separated list of paging-dn-tags that have previously been associated with the paging extension of a paging set using the **paging-dn** command. You can include up to ten paging-dn-tags separated by commas; for example, 4, 6, 7, 8.
Step 8	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 9	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn configuration mode. • *dn-tag*—Unique sequence number that identifies a particular directory number during configuration tasks. Range is 1 to 150 or the maximum defined by the **max-dn** command.

	Command or Action	Purpose
Step 10	**number** *number* **Example:** `Router(config-register-dn)# number 1201`	Associates a telephone or extension number with a Cisco Unified SIP IP phone in a Cisco Unified CME system. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally, the string is composed of digits, but the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number.
Step 11	**exit** **Example:** `Router(config-register-dn)# exit`	Exits voice register dn configuration mode.
Step 12	Repeat Step 9 to Step 11 to associate more telephone or extension numbers with Cisco Unified SIP IP phones.	—
Step 13	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 1`	Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME. • *pool-tag*—Unique number assigned to the pool. Range: 1 to 100. **Note** For Cisco Unified CME systems, the upper limit for this argument is defined by the **max-pool** command.
Step 14	**id mac** *address* **Example:** `Router(config-register-pool)# id mac 0019.305D.82B8`	identifies a locally available Cisco Unified SIP IP phone. • **mac** *address*—identifies the MAC address of a particular Cisco Unified SIP IP phone.
Step 15	**type** *phone-type* **Example:** `Router(config-register-pool)# type 7961`	Defines a phone type for a Cisco Unified SIP IP phone. • *phone-type*—Type of Cisco Unified SIP IP phone that is being defined.
Step 16	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 1`	Indicates the E.164 phone numbers that the registrar permits to handle the Register message from the Cisco Unified SIP IP phone. • *tag*—identifies the telephone number when there are multiple number commands. Range: 1 to 10. • **dn** *dn-tag*—identifies the directory number tag for this phone number as defined by the **voice register dn** command. Range: 1 to 150.
Step 17	**paging-dn** *paging-dn-tag* **Example:** `Router(config-register-pool)# paging-dn 20`	Registers a Cisco Unified SIP IP phone to an ephone-dn paging directory number. • *paging-dn-tag*—Ephone-dn tag designated as the paging ephone-dn to which a Cisco Unified SIP IP phone is registered.

	Command or Action	Purpose
Step 18	Repeat Step 13 to Step 17 to register additional Cisco Unified SIP IP phones to ephone-dn paging directory numbers. Exit from voice register pool configuration mode after each additional phone is registered. After the last phone is added, go directly to Step 19.	—
Step 19	**end** **Example:** `Router(config-register-pool)# end`	Exits voice register pool configuration mode and enters privileged EXEC mode.

Troubleshooting Tips

Use the **debug ephone paging** command to collect debugging information on paging for both Cisco Unified SIP IP and Cisco Unified SCCP IP phones.

Verify Paging

Step 1 Use the **show running-config** command to display the running configuration. Paging ephone-dns are listed in the ephone-dn portion of the output. Phones that belong to paging groups are listed in the ephone part of the output.

```
Router# show running-config

ephone-dn  48
 number 136
 name PagingCashiers
 paging ip 239.1.1.10 port 2000

ephone  2
 headset auto-answer line 1
 headset auto-answer line 4
 ephone-template 1
 username "FrontCashier"
 mac-address 011F.2A0.A490
 paging-dn 48
 type 7960
 no dnd feature-ring
 no auto-line
 button  1f43 2f44 3f45 4:31
```

Step 2 Use the **show telephony-service ephone-dn** and **show telephony-service ephone** commands to display only the configuration information for ephone-dns and ephones.

Configuration Examples for Paging

Example for Configuring Simple Paging Group

The following example sets up an ephone-dn for multicast paging. This example creates a paging number for 5001 on ephone-dn 22 and adds ephone 4 as a member of the paging set. Multicast is set for the paging-dn.

```
ephone-dn 22
 name Paging Shipping
 number 5001
 paging ip 239.1.1.10 port 2000

ephone 4
 mac-address 0030.94c3.8724
 button 1:1 2:2
 paging-dn 22 multicast
```

In this example, paging calls to 2000 are multicast to Cisco Unified IP phones 1 and 2, and paging calls to 2001 go to Cisco Unified IP phones 3 and 4. Note that the paging ephone-dns (20 and 21) are not assigned to any phone buttons.

```
ephone-dn 20
 number 2000
 paging ip 239.0.1.20 port 2000

ephone-dn 21
 number 2001
 paging ip 239.0.1.21 port 2000

ephone 1
 mac-address 3662.024.6ae2
 button 1:1
 paging-dn 20

ephone 2
 mac-address 9387.678.2873
 button 1:2
 paging-dn 20

ephone 3
 mac-address 0478.2a78.8640
 button 1:3
 paging-dn 21

ephone 4
 mac-address 4398.b694.456
 button 1:4
 paging-dn 21
```

Example for Configuring Combined Paging Groups

This example sets the following paging behavior:

- When extension 2000 is dialed, a page is sent to ephones 1 and 2 (single paging group).
- When extension 2001 is dialed, a page is sent to ephones 3 and 4 (single paging group).

- When extension 2002 is dialed, a page is sent to ephones 1, 2, 3, 4, and 5 (combined paging group).

Ephones 1 and 2 are included in paging ephone-dn 22 through the membership of ephone-dn 20 in the combined paging group. Ephones 3 and 4 are included in paging ephone-dn 22 through membership of ephone-dn 21 in the combined paging group. Ephone 5 is directly subscribed to paging-dn 22.

```
ephone-dn 20
 number 2000
 paging ip 239.0.1.20 port 2000

ephone-dn 21
 number 2001
 paging ip 239.0.1.21 port 2000

ephone-dn 22
 number 2002
 paging ip 239.0.2.22 port 2000
 paging group 20,21

ephone-dn 6
 number 1103
 name user3

ephone-dn 7
 number 1104
 name user4

ephone-dn 8
 number 1105
 name user5

ephone-dn 9
 number 1199

ephone-dn 10
 number 1198

ephone 1
 mac-address 1234.8903.2941
 button 1:6
 paging-dn 20

ephone 2
 mac-address CFBA.321B.96FA
 button 1:7
 paging-dn 20

ephone 3
 mac-address CFBB.3232.9611
 button 1:8
 paging-dn 21

ephone 4
 mac-address 3928.3012.EE89
 button 1:9
 paging-dn 21

ephone 5
 mac-address BB93.9345.0031
 button 1:10
 paging-dn 22
```

Example for Configuring a Combined Paging Group of Cisco Unified SIP IP Phones and Cisco Unified SCCP IP Phones

The following example shows how to configure a combined paging group composed of Cisco Unified SIP IP phones and Cisco Unified SCCP IP phones.

In the following configuration tasks, paging sets 20 and 21 are defined and then combined into paging group 22. Paging set 20 has a paging extension of 2000. When someone dials extension 2000 to deliver a page, the page is sent to Cisco Unified SCCP IP phones (ephones) 1 and 2. Paging set 21 has a paging extension of 2001. When someone dials extension 2001 to deliver a page, the page is sent to ephones 3 and 4. Paging group 22 combines sets 20 and 21, and when someone dials its paging extension, 2002, the page is sent to all the phones in both sets and to ephone 5, which is directly subscribed to the combined paging group.

```
ephone-dn 20
 number 2000
 paging ip 239.0.1.20 port 2000

ephone-dn 21
 number 2001
 paging ip 239.0.1.21 port 2000

ephone-dn 22
 number 2002
 paging ip 239.0.2.22 port 2000
 paging group 20,21

ephone 1
 button 1:1
 paging-dn 20

ephone 2
 button 1:2
 paging-dn 20

ephone 3
 button 1:3
 paging-dn 21

ephone 4
 button 1:4
 paging-dn 21

ephone 5
 button 1:5
 paging-dn 22
```

The following configuration tasks show how to configure a combined paging group composed of Cisco Unified SCCP IP phone directory numbers only.

When extension 2000 is dialed, a page is sent to ephones 1 and 2 (first single paging group). When extension 2001 is dialed, a page is sent to ephones 3 and 4 (second single paging group). Finally, when extension 2002 is dialed, a page is sent to ephones 1, 2, 3, 4, and 5, producing the combined paging group (composed of the first single paging group, the second single paging group, and ephone 5).

Ephones 1 and 2 are included in paging ephone-dn 22 through the membership of ephone-dn 20 as paging group 20 in the combined paging group. Ephones 3 and 4 are included in paging ephone-dn 22 through membership of ephone-dn 21 as paging group 21 in the combined paging group. Ephone 5 is directly subscribed to paging-dn 22.

```
ephone-dn 20
```

```
 number 2000
 paging ip 239.0.1.20 port 20480

ephone-dn 21
 number 2001
 paging ip 239.1.1.21 port 20480

ephone-dn 22
 number 2002
 paging ip 239.1.1.22 port 20480
 paging group 20,21

ephone-dn 6
 number 1103

ephone-dn 7
 number 1104

ephone-dn 8
 number 1105

ephone-dn 9
 number 1199

ephone-dn 10
 number 1198

ephone 1
 mac-address 1234.8903.2941
 button 1:6
 paging-dn 20

ephone 2
 mac-address CFBA.321B.96FA
 button 1:7
 paging-dn 20

ephone 3
 mac-address CFBB.3232.9611
 button 1:8
paging-dn 21

ephone 4
 mac-address 3928.3012.EE89
 button 1:9
 paging-dn 21

ephone 5
 mac-address BB93.9345.0031
 button 1:10
 paging-dn 22
```

In the following configuration tasks, the **paging group** command is used to configure combined paging groups composed of ephone and voice register directory numbers.

When extension 2000 is dialed, a page is sent to ephones 1 and 2 and voice register pools 1 and 2 (new first single paging group). When extension 2001 is dialed, a page is sent to ephones 3 and 4 and voice register pools 3 and 4 (new second single paging group). Finally, when extension 2002 is dialed, a page is sent to ephones 1, 2, 3, 4, and 5 and voice register pools 1, 2, 3, 4, and 5 (new combined paging group).

Ephones 1 and 2 and voice register pools 1 and 2 are included in paging ephone-dn 22 through the membership of ephone-dn 20 as paging group 20 in the combined paging group. Ephones 3 and 4 and voice register pools 3 and 4 are included in paging ephone-dn 22 through membership of ephone-dn 21 as paging group 21 in the combined paging group. Ephone 5 and voice register pool 5 are directly subscribed to paging-dn 22.

```
voice register dn 1
 number 1201
```

```
voice register dn 2
 number 1202

voice register dn 3
 number 1203

voice register dn 4
 number 1204

voice register dn 5
 number 1205

voice register pool 1
 id mac 0019.305D.82B8
 type 7961
 number 1 dn 1
paging-dn 20

voice register pool  2
 id mac 0019.305D.2153
 type 7961
 number 1 dn 2
 paging-dn 20

voice register pool  3
 id mac 1C17.D336.58DB
 type 7961
 number 1 dn 3
 paging-dn 21

voice register pool  4
 id mac 0017.9437.8A60
 type 7961
 number 1 dn 4
 paging-dn 21

voice register pool  5
 id mac 0016.460D.E469
 type 7961
 number 1 dn 5
 paging-dn 22
```

Where to Go Next

Intercom

The intercom feature is similar to paging because it allows a phone user to deliver an audio message to a phone without the called party having to answer. The intercom feature is different than paging because the audio path between the caller and the called party is a dedicated audio path and because the called party can respond to the caller. See Intercom Lines, on page 783.

Speed Dial

Phone users who make frequent pages may want to include the paging ephone-dn numbers in their list of speed-dial numbers. See Speed Dial, on page 965.

Feature Information for Paging

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

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

Table 71: Feature Information for Paging

Feature Name	Cisco Unified CME Version	Feature Information
Paging	2.0	Paging was introduced.
Paging Group Support for Cisco Unified SIP IP Phones	9.0	Allows you to specify a paging-dn tag and dial the paging extension number to page the Cisco Unified SIP IP phone associated with the paging-dn tag or paging group using the **paging-dn** command in voice register pool or voice register template configuration mode.

CHAPTER 31

Presence Service

Prerequisites for Presence Service

- Cisco Unified CME 4.1 or a later version.

Restrictions for Presence Service

- Presence features such as Busy Lamp Field (BLF) notification are supported for SIP trunks only; these features are not supported on H.323 trunks.
- Presence requires that SIP phones are configured with a directory number (using **dn** keyword in **number** command); direct line numbers are not supported.

Information About Presence Service

Presence Service

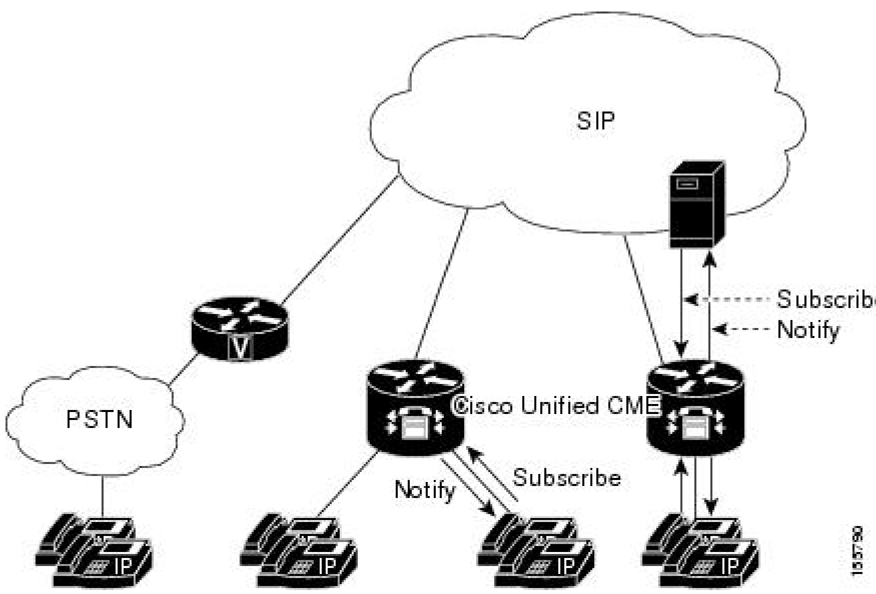
A presence service, as defined in RFC 2778 and RFC 2779, is a system for finding, retrieving, and distributing presence information from a source, called a presence entity (presentity), to an interested party called a watcher. When you configure presence in a Cisco Unified CME system with a SIP WAN connection, a phone user, or watcher, can monitor the real-time status of another user at a directory number, the presentity. Presence enables the calling party to know before dialing whether the called party is available. For example, a directory application may show that a user is busy, saving the caller the time and inconvenience of not being able to reach someone.

Presence uses SIP SUBSCRIBE and NOTIFY methods to allow users and applications to subscribe to changes in the line status of phones in a Cisco Unified CME system. Phones act as watchers and a presentity is identified by a directory number on a phone. Watchers initiate presence requests (SUBSCRIBE messages) to obtain the line status of a presentity. Cisco Unified CME responds with the presentity's status. Each time a status changes for a presentity, all watchers of this presentity are sent a notification message. SIP phones and trunks use SIP messages; SCCP phones use presence primitives in SCCP messages.

Presence supports Busy Lamp Field (BLF) notification features for speed-dial buttons and directory call lists for missed calls, placed calls, and received calls. SIP and SCCP phones that support the BLF speed-dial and BLF call-list features can subscribe to status change notification for internal and external directory numbers.

Figure 36: BLF Notification Using Presence shows a Cisco Unified CME system supporting BLF notification for internal and external directory numbers. If the watcher and the presentity are not both internal to the Cisco Unified CME router, the subscribe message is handled by a presence proxy server.

Figure 36: BLF Notification Using Presence



The following line states display through BLF indicators on the phone:

- Line is idle—Displays when this line is not being used.
- Line is in-use—Displays when the line is in the ringing state and when a user is on the line, whether or not this line can accept a new call.
- BLF indicator unknown—Phone is unregistered or this line is not allowed to be watched.

Cisco Unified CME acts as a presence agent for internal lines (both SIP and SCCP) and as a presence server for external watchers connected through a SIP trunk, providing the following functionality:

- Processes SUBSCRIBE requests from internal lines to internal lines. Notifies internal subscribers of any status change.

- Processes incoming SUBSCRIBE requests from a SIP trunk for internal SCCP and SIP lines. Notifies external subscribers of any status change.
- Sends SUBSCRIBE requests to external presentities on behalf of internal lines. Relays status responses to internal lines.

Presence subscription requests from SIP trunks can be authenticated and authorized. Local subscription requests cannot be authenticated.

For configuration information, see Configure Presence Service.

BLF Monitoring of Ephone-DNs with DnD, Call Park, Paging, and Conferencing

In versions earlier than Cisco Unified CME 7.1, BLF monitoring does not provide notification of status changes when a monitored directory number becomes DND-enabled, and the Busy Lamp Field (BLF) indicators for directory numbers configured as call-park slots, paging numbers, or ad hoc or meet-me conference numbers display only the unknown line-status.

Cisco Unified CME 7.1 and later versions support idle, in-use, and unknown BLF status indicators for monitored ephone-dns configured as call-park slots, paging numbers, and ad hoc or meet-me conference numbers. This allows an administrator (watcher) to monitor a call-park slot to see if calls are parked and not yet retrieved, which paging number is available for paging, or which conference number is available for a conference.

An ephone-dn configured as a park-slot is not registered with any phone. In Cisco Unified CME 7.1 and later versions, if a monitored park-slot is idle, the BLF status shows idle on the watcher. If there is a call parked on the monitored park-slot, the BLF status indicates in-use. If the monitored park-slot is not enabled for BLF monitoring with the **allow watch** command, the BLF indicator for unknown status displays on the watcher.

An ephone-dn configured for paging or conferencing is also not registered with any phone. The indicators for the idle, in-use, and unknown BLF status are displayed for the monitored paging number and ad hoc or meet-me conference numbers, as with the call-park slots.

Cisco Unified CME 7.1 and later versions support the Do Not Disturb (DnD) BLF status indicator for ephone-dns in the DnD state. When a user presses the DnD softkey on an SCCP phone, all directory numbers assigned to the phone become DnD-enabled and a silent-ring is played for all calls to any directory number on the phone. If a monitored ephone-dn becomes DnD-enabled, the corresponding BLF speed-dial lamp (if available) on the watcher displays solid red with the DnD icon for both the idle and in-use BLF status.

The BLF status notification occurs if the monitored ephone-dn is:

- The primary directory number on only one SCCP phone
- A directory number that is not shared
- A shared directory number and all associated phones are DnD-enabled

No new configuration is required to support these enhancements. For information on configuring BLF monitoring of directory numbers, see Enable BLF Monitor for Speed-Dials and Call Lists Using SCCP Phones.

Table 72: Feature Comparison of Directory Number BLF Monitoring compares the different BLF monitoring features that can be configured in Cisco Unified CME.

Table 72: Feature Comparison of Directory Number BLF Monitoring

Monitor Mode (Button "m")	Watch Mode (Button "w")	BLF Monitoring
Basic Operation		
SCCP phones only. Watches a single ephone-dn instance. If there are multiple ephone-dns with the same extension (such as in an overlay), this mode watches only a single ephone-dn (specified with the **button** command using m keyword). Does not indicate DND state of the phone.	SCCP phones only. Watches all activity on the phone for which the designated ephone-dn is the primary extension. (The ephone-dn is "primary" for a phone if the extension appears on button 1 or on the button indicated by the **auto-line** command.) Ephone-dn can be shared but cannot be the primary extension on any other phone. Indicates DND state of the phone.	SCCP and SIP phones. Watches all ephone-dn instances with the same (primary) extension number. The BLF lamp is on if any instance of the monitored extension is in use. Indicates DND state of the phone.
Shared Lines		
Can not distinguish which phone is using the ephone-dn if the DN is shared across multiple phones.	Designed for cases where ephone-dns are shared across multiple phones. Each phone must have a unique primary ephone-dn. Used to indicate that a specific phone is in use as opposed (button m) to indicating that a specific ephone-dn is in use.	Cannot distinguish which phone is using the ephone-dn, if the DN is shared across multiple phones.
Local vs. Remote		
Monitors only DNs on the local Cisco Unified CME system.	Can only monitor DNs that are on the local Cisco Unified CME system	Can monitor extension numbers on a remote Cisco Unified CME using SIP Subscribe and Notify. Cannot monitor local and remote at the same time.

Device-Based BLF Monitoring

Device-based BLF monitoring provides a phone user or administrator (watcher) information about the status of a monitored phone (presentity). Cisco Unified CME 4.1 and later versions support BLF monitoring of directory numbers associated with speed-dial buttons, call logs, and directory listings. Cisco Unified CME 7.1 and later versions support device-based BLF monitoring, allowing a watcher to monitor the status of a phone, not only a line on the phone.

To identify the phone being monitored for BLF status, Cisco Unified CME selects the phone with the monitored directory number assigned to the first button, or the directory number whose button is selected by the **auto-line** command (SCCP only). If more than one phone uses the same number as its primary directory number, the phone with the lowest phone tag is monitored for BLF status.

For Extension Mobility phones, the first number configured in the user profile indicates the primary directory number of the Extension Mobility phone. If the Extension Mobility phone is being monitored, the BLF status of the corresponding phone is sent to the watcher when an extension-mobility user logs in or out, is idle, or busy.

If a shared directory number is busy on a monitored SCCP phone, and the monitored device is on-hook, the monitored phone is considered idle.

When a monitored phone receives a page, if the paging directory number is also monitored, the BLF status of the paging directory number shows busy on the watcher.

If device-based monitoring is enabled on a directory number configured as a call-park slot, and there is a call parked on this park-slot, the device-based BLF status indicates busy.

All directory numbers associated with a phone are in the DnD state when the DnD softkey is pressed. If a monitored phone becomes DnD-enabled, watchers are notified of the DnD status change.

For configuration information, see Enable BLF Monitor for Speed-Dials and Call Lists Using SCCP Phones or Enable BLF Monitoring for Speed-Dials and Call Lists on SIP Phones.

Phone User Interface for BLF-Speed-Dial

Cisco Unified CME 8.5 and later versions allows the extension mobility (EM) users to configure dn-based Busy Lamp Field (BLF)-speed-dial settings directly on the phone through the services feature button. BLF-speed-dial settings are added or modified (changed or deleted) on the phone using a menu available with the Services button. Any changes to the BLF-speed-dial settings made through the phone user interface are applied to the user's profile in extension mobility. You can configure the BLF-speed-dial menu for SCCP phones using the **blf-speed-dial** command in ephone or ephone-template mode. For more information, see Enable BLF-Speed-Dial Menu.

For information on how phone users configure BLF-speed-dial using the phone user-interface, see the Cisco Unified IP Phone documentation for Cisco Unified CME .

For phones that do not have EM feature, the BLF-speed-dial service is available in service url page. You can disable the BLF-speed- dial feature using the **no phone-ui blf-speed-dial** command on phones that do not have Extension Mobility.

Configure Presence Service

Enable Presence for Internal Lines

Perform the following steps to enable the router to accept incoming presence requests from internal watchers and SIP trunks.

Restriction

- A presentity can be identified by a directory number only.
- BLF monitoring indicates the line status only.
- Instant Messaging is not supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **presence enable**
5. **exit**
6. **presence**
7. **max-subscription** *number*
8. **presence call-list**
9. **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	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode to configure the user agent.
Step 4	**presence enable** **Example:** `Router(config-sip-ua)# presence enable`	Allows the router to accept incoming presence requests.
Step 5	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits SIP user-agent configuration mode.

	Command or Action	Purpose
Step 6	**presence** **Example:** `Router(config)# presence`	Enables presence service and enters presence configuration mode.
Step 7	**max-subscription** *number* **Example:** `Router(config-presence)# max-subscription 128`	(Optional) Sets the maximum number of concurrent watch sessions that are allowed. • *number*—Maximum watch sessions. Range: 100 to the maximum number of directory numbers supported on the router platform. Type **?** to display range. Default: 100.
Step 8	**presence call-list** **Example:** `Router(config-presence)# presence call-list`	Globally enables BLF monitoring for directory numbers in call lists and directories on all locally registered phones. • Only directory numbers that you enable for watching with the **allow watch** command display BLF status indicators. • This command enables the BLF call-list feature globally. To enable the feature for a specific phone, see Enable BLF Monitor for Speed-Dials and Call Lists Using SCCP Phones.
Step 9	**end** **Example:** `Router(config-presence)# end`	Exits to privileged EXEC mode.

Enable a Directory Number to be Watched

To enable a line associated with a directory number to be monitored by a phone registered to a Cisco Unified CME router, perform the following steps. The line is enabled as a presentity and phones can subscribe to its line status through the BLF call-list and BLF speed-dial features. There is no restriction on the type of phone that can have its lines monitored; any line on any IP phone or on an analog phone on supported voice gateways can be a presentity.

Restriction

- A presentity is identified by a directory number only.
- BLF monitoring indicates the line status only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**] or **voice register dn** *dn-tag*
4. **number** *number*
5. **allow watch**
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	**ephone-dn** *dn-tag* [**dual-line**] or **voice register dn** *dn-tag*
	
	Example:
	`Router(config)# ephone-dn 1`
	or
	`Router(config)# voice register dn 1`
		Enters the configuration mode to define a directory number for an IP phone, intercom line, voice port, or a message-waiting indicator (MWI).
		• *dn-tag*—identifies a particular directory number during configuration tasks. Range is 1 to the maximum number of directory numbers allowed on the router platform, or the maximum defined by the **max-dn** command. Type **?** to display range.

Step 4	**number** *number*
	
	Example:
	`Router(config-ephone-dn)# number 3001`
	or
	`Router(config-register-dn)# number 3001`
		Associates a phone number with a directory number to be assigned to an IP phone in Cisco Unified CME.
		• *number*—String of up to 16 characters that represents an E.164 telephone number.

Step 5	**allow watch**
	
	Example:
	`Router(config-ephone-dn)# allow watch`
	or
	`Router(config-register-dn)# allow watch`
		Allows the phone line associated with this directory number to be monitored by a watcher in a presence service.
		• This command can also be configured in ephone-dn template configuration mode and applied to one or more phones. The ephone-dn configuration has priority over the ephone-dn template configuration.

	Command or Action	Purpose

Step 6	**end**
	
	Example:
	`Router(config-ephone-dn)# end`
	or
	`Router(config-register-dn)# end`
		Exits to privileged EXEC mode.

Enable BLF Monitor for Speed-Dials and Call Lists Using SCCP Phones

A watcher can monitor the status of lines associated with internal and external directory numbers (presentities) through the BLF speed-dial and BLF call-list presence features. To enable the BLF notification features on an IP phone using SCCP, perform the following steps.

Restriction

- Device-based BLF monitoring for call lists is not supported.
- Device-based BLF-speed-dial monitoring is not supported for a remote watcher or presentity.

BLF Call-List

- Not supported on Cisco Unified IP Phone 7905, 7906, 7911, 7912, 7931, 7940, 7960, or 7985, Cisco Unified IP Phone Expansion Modules, or Cisco Unified IP Conference Stations.

BLF Speed-Dial

- Not supported on Cisco Unified IP Phone 7905, 7906, 7911, 7912, or 7985, or Cisco Unified IP Conference Stations.

Cisco Unified IP Phone 7931

- BLF status is displayed through monitor lamp only; BLF status icons are not displayed.

Before You Begin

- Presence must be enabled on the Cisco Unified CME router. See Enable Presence for Internal Lines.
- A directory number must be enabled as a presentity with the **allow watch** command to provide BLF status notification. See Enable a Directory Number to be Watched.
- Device-based monitoring requires Cisco Unified CME 7.1 or a later version. All directory numbers associated with the monitored phone must be configured with the **allow watch** command. Otherwise, if any of the directory numbers is missing this configuration, an incorrect status could be reported to the watcher.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **button** *button-number* {*separator*} *dn-tag* [**,***dn-tag*...] [*button-number*{**x**}*overlay-button-number*] [*button-number***...**]
5. **blf-speed-dial** *tag number* **label** *string* [**device**]
6. **presence call-list**
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	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode to set phone-specific parameters for a SIP phone. • *phone-tag*—Unique sequence number of the phone to be configured. Range is version and platform-dependent; type **?** to display range. You can modify the upper limit for this argument with the **max-ephones** command.
Step 4	**button** *button-number* {*separator*} *dn-tag* [**,***dn-tag*...] [*button-number*{**x**}*overlay-button-number*] [*button-number***...**] **Example:** `Router(config-ephone)# button 1:10 2:11 3b12 4o13,14,15`	Associates a button number and line characteristics with a directory number on the phone. • *button-number*—Number of a line button on an IP phone. • *separator*—Single character that denotes the type of characteristics to be associated with the button. • *dn-tag*—Unique sequence number of the ephone-dn that you want to appear on this button. For overlay lines (separator is **o** or**c**), this argument can contain up to 25 ephone-dn tags, separated by commas. • **x**—Separator that creates an overlay rollover button. • *overlay-button-number*—Number of the overlay button that should overflow to this button.

	Command or Action	Purpose
Step 5	**blf-speed-dial** *tag number* **label** *string* [**device**] **Example:** `Router(config-ephone)# blf-speed-dial 3 3001 label sales device`	Enables BLF monitoring of a directory number associated with a speed-dial number on the phone. • *tag*—Number that identifies the speed-dial index. Range: 1 to 33. • *number*—Telephone number to speed dial. • *string*—Alphanumeric label that identifies the speed-dial button. String can contain a maximum of 30 characters. • **device**—(Optional) Enables phone-based monitoring. This keyword is supported in Cisco Unified CME 7.1 and later versions.
Step 6	**presence call-list** **Example:** `Router(config-ephone)# presence call-list`	Enables BLF monitoring of directory numbers that appear in call lists and directories on this phone. • For a directory number to be monitored, it must have the allow watch command enabled. • To enable BLF monitoring for call lists on all phones in this Cisco Unified CME system, use this command in presence mode. See Enable Presence for Internal Lines, on page 879.
Step 7	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

The following example shows that the directory numbers for extensions 2001 and 2003 are allowed to be watched and the BLF status of these numbers display on phone 1.

```
ephone-dn  201
number 2001
allow watch
!
!
ephone-dn  203
number 2003
allow watch
!
!
ephone  1
mac-address 0012.7F54.EDC6
blf-speed-dial 2 201 label "sales" device
blf-speed-dial 3 203 label "service" device
button  1:100 2:101 3b102
```

What to Do Next

If you are done modifying parameters for SCCP phones in Cisco Unified CME, generate a new configuration profile by using the **create cnf-files** command and then restart the phones with the **restart** command. See Generate Configuration Files for SCCP Phones and Use the restart Command on SCCP Phones.

Enable BLF Monitoring for Speed-Dials and Call Lists on SIP Phones

A watcher can monitor the status of lines associated with internal and external directory numbers (presentities) through the BLF speed-dial and BLF call-list presence features. To enable the BLF notification features on a SIP phone, perform the following steps.

Restriction

- Device-based BLF-speed-dial monitoring is not supported for a remote watcher or presentity.
- TCP based, device-based BLF-speed-dial monitoring is not supported on Unified CME.

BLF Call-List

- Not supported on Cisco Unified IP Phone 7905, 7906, 7911, 7912, 7931, 7940, 7960, or 7985, Cisco Unified IP Phone Expansion Modules, or Cisco Unified IP Conference Stations.

BLF Speed-Dial

- Not supported on Cisco Unified IP Phone 7905, 7906, 7911, 7912, or 7985, or Cisco Unified IP Conference Stations.

Before You Begin

- Presence must be enabled on the Cisco Unified CME router. See Enable Presence for Internal Lines.
- A directory number must be enabled as a presentity with the **allow watch** command to provide BLF status notification. See Enable a Directory Number to be Watched.
- SIP phones must be configured with a directory number under voice register pool configuration mode (use **dn** keyword in **number** command); direct line numbers are not supported.
- Device-based monitoring requires Cisco Unified CME 7.1 or a later version. All directory numbers associated with the monitored phone must be configured with the **allow watch** command. Otherwise, if any of the directory numbers is missing this configuration, an incorrect status could be reported to the watcher.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **number** *tag* **dn** *dn-tag*
5. **blf-speed-dial** *tag number* **label** *string* [**device**]
6. **presence call-list**
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 register pool** *pool-tag* **Example:** `Router(config)# voice register pool 1`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone. • *pool-tag*—Unique sequence number of the SIP phone to be configured. Range is version and platform-dependent; type **?** to display range. You can modify the upper limit for this argument with the **max-pool** command.
Step 4	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 2`	Assigns a directory number to the SIP phone. • tag—identifier when there are multiple **number** commands. Range: 1 to 10. • *dn-tag*—Directory number tag that was defined using the **voice register dn** command.
Step 5	**blf-speed-dial** *tag number* **label** *string* [**device**] **Example:** `Router(config-register-pool)# blf-speed-dial 3 3001 label sales device`	Enables BLF monitoring of a directory number associated with a speed-dial number on the phone. • *tag*—Number that identifies the speed-dial index. Range: 1 to 7. • *number*—Telephone number to speed dial. • *string*—Alphanumeric label that identifies the speed-dial button. The string can contain a maximum of 30 characters. • **device**—(Optional) Enables phone-based monitoring. This keyword is supported in Cisco Unified CME 7.1 and later versions.
Step 6	**presence call-list** **Example:** `Router(config-register-pool)# presence call-list`	Enables BLF monitoring of directory numbers that appear in call lists and directories on this phone. • For a directory number to be monitored, it must have the **allow watch** command enabled. • To enable BLF monitoring for call lists on all phones in this Cisco Unified CME system, use this command in presence mode. See Enable Presence for Internal Lines.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.

What to Do Next

If you are done modifying parameters for SIP phones in Cisco Unified CME, generate a new configuration profile by using the **create profile** command and then restart the phones with the **restart** command. See Generate Configuration Profiles for SIP Phones and Use the restart Command on SIP Phones.

Enable BLF-Speed-Dial Menu

Restriction

- EM user cannot modify the logout profile from phone user interface (UI).
- Extension Mobility (EM) users must log into EM profile to update BLF-speed-dial number.

Before You Begin

- Cisco Unified CME 8.5 or later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **blf-speed-dial** [**index** *index number*] [**phone-number** *number*] [**label** *label text*]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 10`	Enters ephone configuration mode. • phone-tag—Unique number of the phone for which you want to configure BLF-speed-dial numbers.
Step 4	**blf-speed-dial** [**index** *index number*] [**phone-number** *number*] [**label** *label text*] **Example:** `Router(config-ephone)#blf-speed-dial 1 2001 label "customer support"`	Creates an entry for a BLF-speed-dial number on this phone. • BLF-speed-dial index—Unique identifier to identify this entry during configuration. Range is 1 to 75. • phone number—Telephone number or extension to be dialed.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Configure Presence to Watch External Lines

To enable internal watchers to monitor external directory numbers on a remote Cisco Unified CME router, perform the following steps.

Before You Begin

Presence service must be enabled for internal lines. See Enable Presence for Internal Lines.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **presence**
4. **server** *ip-address*
5. **allow subscribe**
6. **watcher all**
7. **sccp blf-speed-dial retry-interval** *seconds* **limit** *number*
8. **exit**
9. **voice register global**
10. **authenticate presence**
11. **authenticate credential** *tag location*
12. **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	**presence** **Example:** `Router(config)# presence`	Enables presence service and enters presence configuration mode.
Step 4	**server** *ip-address* **Example:** `Router(config-presence)# server 10.10.10.1`	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presentities.
Step 5	**allow subscribe** **Example:** `Router(config-presence)# allow subscribe`	Allows internal watchers to monitor external directory numbers.
Step 6	**watcher all** **Example:** `Router(config-presence)# watcher all`	Allows external watchers to monitor internal directory numbers.

	Command or Action	Purpose
Step 7	**sccp blf-speed-dial retry-interval** *seconds* **limit** *number* **Example:** `Router(config-presence)# sccp blf-speed-dial retry-interval 90 limit number 15`	(Optional) Sets the retry timeout for BLF monitoring of speed-dial numbers on phones running SCCP. • *seconds*—Retry timeout in seconds. Range: 60 to 3600. Default: 60. • *number*—Maximum number of retries. Range: 10 to 100. Default: 10.
Step 8	**exit** **Example:** `Router(config-presence)# exit`	Exits presence configuration mode.
Step 9	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set global parameters for all supported SIP phones in a Cisco Unified CME environment.
Step 10	**authenticate presence** **Example:** `Router(config-register-global)# authenticate presence`	(Optional) Enables authentication of incoming presence requests from a remote presence server.
Step 11	**authenticate credential** *tag location* **Example:** `Router(config-register-global)# authenticate credential 1 flash:cred1.csv`	(Optional) Specifies the credential file to use for authenticating presence subscription requests. • *tag*—Number that identifies the credential file to use for presence authentication. Range: 1 to 5. • *location*—Name and location of the credential file in URL format. Valid storage locations are TFTP, HTTP, and flash memory.
Step 12	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Verify Presence Configuration

Step 1 **show running-config**

Use this command to verify your configuration.

Router# **show running-config**
```
!
voice register global
 mode cme
 source-address 10.1.1.2 port 5060
 load 7971 SIP70.8-0-1-11S
 load 7970 SIP70.8-0-1-11S
 load 7961GE SIP41.8-0-1-0DEV
 load 7961 SIP41.8-0-1-0DEV
 authenticate presence
 authenticate credential 1 tftp://172.18.207.15/labtest/cred1.csv
 create profile sync 0004550081249644
.
.
.
presence
 server 10.1.1.4
 sccp blf-speed-dial retry-interval 70 limit 20
 presence call-list
 max-subscription 128
 watcher all
 allow subscribe
!
sip-ua
 presence enable
```

Step 2 **show presence global**

Use this command to display presence configuration settings.

Router# **show presence global**

```
Presence Global Configuration Information:
=============================================
Presence feature enable           : TRUE
Presence allow external watchers  : FALSE
Presence max subscription allowed : 100
Presence number of subscriptions  : 0
Presence allow external subscribe : FALSE
Presence call list enable         : TRUE
Presence server IP address        : 0.0.0.0
Presence sccp blfsd retry interval : 60
Presence sccp blfsd retry limit   : 10
Presence router mode              : CME mode
```

Step 3 **show presence subscription** [**details** |**presentity** *telephone-number* | **subid** *subscription-id* **summary**]

Use this command to display information about active presence subscriptions.

Router# **show presence subscription summary**

```
Presence Active Subscription Records Summary: 15 subscription
Watcher                  Presentity              SubID Expires SibID  Status
```

```
======================= ======================= ====== ======= ====== ======
6002@10.4.171.60        6005@10.4.171.34        1 3600    0      idle
6005@10.4.171.81        6002@10.4.171.34        6 3600    0      idle
6005@10.4.171.81        6003@10.4.171.34        8 3600    0      idle
6005@10.4.171.81        6002@10.4.171.34        9 3600    0      idle
6005@10.4.171.81        6003@10.4.171.34        10 3600    0      idle
6005@10.4.171.81        6001@10.4.171.34        12 3600    0      idle
6001@10.4.171.61        6003@10.4.171.34        15 3600    0      idle
6001@10.4.171.61        6002@10.4.171.34        17 3600    0      idle
6003@10.4.171.59        6003@10.4.171.34        19 3600    0      idle
6003@10.4.171.59        6002@10.4.171.34        21 3600    0      idle
6003@10.4.171.59        5001@10.4.171.34        23 3600    24     idle
6002@10.4.171.60        6003@10.4.171.34        121 3600    0      idle
6002@10.4.171.60        5002@10.4.171.34        128 3600    129    idle
6005@10.4.171.81        1001@10.4.171.34        130 3600    131    busy
6005@10.4.171.81        7005@10.4.171.34        132 3600    133    idle
```

Troubleshooting Presence Service

You can use the following commands to troubleshoot presence service:

- **debug presence** {**all** | **asnl** |**errors** | **event** | **info** | **timer** | **trace** | **xml**}
- **debug ephone blf** [**mac-address** *mac-address*]

Configuration Examples for Presence Service

Example for Configuring Presence in Cisco Unified CME

```
Router# show running-config

Building configuration...

Current configuration : 5465 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CME-3825
!
boot-start-marker
boot-end-marker
!
logging buffered 2000000 debugging
enable password lab
!
no aaa new-model
!
resource policy
```

```
!
no network-clock-participate slot 1
no network-clock-participate slot 2
ip cef
!
!
no ip domain lookup
!
voice-card 1
no dspfarm
!
voice-card 2
no dspfarm
!
!
voice service voip
allow-connections sip to sip
h323
sip
registrar server expires max 240 min 60
!
voice register global
mode cme
source-address 11.1.1.2 port 5060
load 7971 SIP70.8-0-1-11S
load 7970 SIP70.8-0-1-11S
load 7961GE SIP41.8-0-1-0DEV
load 7961 SIP41.8-0-1-0DEV
authenticate presence
authenticate credential 1 tftp://172.18.207.15/labtest/cred1.csv
create profile sync 0004550081249644
!
voice register dn  1
number 2101
allow watch
!
voice register dn  2
number 2102
allow watch
!
voice register pool  1
id mac 0015.6247.EF90
type 7971
number 1 dn 1
blf-speed-dial 1 1001 label "1001"
!
voice register pool  2
id mac 0012.0007.8D82
type 7912
number 1 dn 2
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 11.1.1.2 255.255.255.0
duplex full
speed 100
media-type rj45
no negotiation auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
media-type rj45
negotiation auto
!
ip route 0.0.0.0 0.0.0.0 11.1.1.1
!
ip http server
!
!
!
```

```
tftp-server flash:Jar41sccp.8-0-0-103dev.sbn
tftp-server flash:cvm41sccp.8-0-0-102dev.sbn
tftp-server flash:SCCP41.8-0-1-0DEV.loads
tftp-server flash:P00303010102.bin
tftp-server flash:P00308000100.bin
tftp-server flash:P00308000100.loads
tftp-server flash:P00308000100.sb2
tftp-server flash:P00308000100.sbn
tftp-server flash:SIP41.8-0-1-0DEV.loads
tftp-server flash:apps41.1-1-0-82dev.sbn
tftp-server flash:cnu41.3-0-1-82dev.sbn
tftp-server flash:cvm41sip.8-0-0-103dev.sbn
tftp-server flash:dsp41.1-1-0-82dev.sbn
tftp-server flash:jar41sip.8-0-0-103dev.sbn
tftp-server flash:P003-08-1-00.bin
tftp-server flash:P003-08-1-00.sbn
tftp-server flash:P0S3-08-1-00.loads
tftp-server flash:P0S3-08-1-00.sb2
tftp-server flash:CP7912080000SIP060111A.sbin
tftp-server flash:CP7912080001SCCP051117A.sbin
tftp-server flash:SCCP70.8-0-1-11S.loads
tftp-server flash:cvm70sccp.8-0-1-13.sbn
tftp-server flash:jar70sccp.8-0-1-13.sbn
tftp-server flash:SIP70.8-0-1-11S.loads
tftp-server flash:apps70.1-1-1-11.sbn
tftp-server flash:cnu70.3-1-1-11.sbn
tftp-server flash:cvm70sip.8-0-1-13.sbn
tftp-server flash:dsp70.1-1-1-11.sbn
tftp-server flash:jar70sip.8-0-1-13.sbn
!
control-plane
!
dial-peer voice 2001 voip
preference 2
destination-pattern 1...
session protocol sipv2
session target ipv4:11.1.1.4
dtmf-relay sip-notify
!
presence
server 11.1.1.4
sccp blf-speed-dial retry-interval 70 limit 20
presence call-list
max-subscription 128
watcher all
allow subscribe
!
sip-ua
authentication username jack password 021201481F
presence enable
!
!
telephony-service
load 7960-7940 P00308000100
load 7941GE SCCP41.8-0-1-0DEV
load 7941 SCCP41.8-0-1-0DEV
load 7961GE SCCP41.8-0-1-0DEV
load 7961 SCCP41.8-0-1-0DEV
load 7971 SCCP70.8-0-1-11S
load 7970 SCCP70.8-0-1-11S
load 7912 CP7912080000SIP060111A.sbin
max-ephones 100
max-dn 300
ip source-address 11.1.1.2 port 2000
url directories http://11.1.1.2/localdirectory
max-conferences 6 gain -6
call-forward pattern .T
transfer-system full-consult
transfer-pattern .T
create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-dn  1  dual-line
```

```
number 2001
allow watch
!
!
ephone-dn  2  dual-line
number 2009
allow watch
application default
!
!
ephone-dn  3
number 2005
allow watch
!
!
ephone-dn  4  dual-line
number 2002
!
!
ephone  1
mac-address 0012.7F57.62A5
fastdial 1 1002
blf-speed-dial 1 2101 label "2101"
blf-speed-dial 2 1003 label "1003"
blf-speed-dial 3 2002 label "2002"
type 7960
button  1:1 2:2
!
!
!
ephone  3
mac-address 0015.6247.EF91
blf-speed-dial 2 1003 label "1003"
type 7971
button  1:3 2:4
!
!
!
line con 0
exec-timeout 0 0
password lab
stopbits 1
line aux 0
stopbits 1
line vty 0 4
password lab
login
!
scheduler allocate 20000 1000
!
end
```

Feature Information for Presence Service

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

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

Table 73: Feature Information for Presence Service

Feature Name	Cisco Unified CME Version	Modification
Phone User Interface for BLF-Speed-Dial	8.5	Added support for BLF Speed Dial through Phone User Interface.
BLF Monitoring	7.1	• Added support for device-based BLF monitoring. • Added support for BLF Monitoring of ephone-DNs with DnD, Call Park, Paging, and Conferencing
Presence Service	4.1	Presence with BLF was introduced.

CHAPTER 32

Ringtones

Information About Ringtones

Distinctive Ringing

Distinctive ring is used to identify internal and external incoming calls. An internal call is defined as a call originating from any Cisco Unified IP phone that is registered in Cisco Unified CME or is routed through the local FXS port.

In Cisco CME 3.4 and earlier versions, the standard ring pattern is generated for all calls to local SCCP endpoints. In Cisco Unified CME 4.0, the following distinctive ring features are supported for SCCP endpoints:

- Specify one of three ring patterns to be used for all types of incoming calls to a particular directory number, on all phones on which the directory number appears. If a phone is already in use, an incoming call is presented as a call-waiting call and uses a distinctive call-waiting beep.
- Specify whether the distinctive ring is used only if the incoming called number matches the primary or secondary number defined for the ephone-dn. If no secondary number is defined for the ephone-dn, the secondary ring option has no effect.
- Associate a feature ring pattern with a specific button on a phone so that different phones that share the same directory number can use a different ring style.

For local SIP endpoints, the type of ring sound requested is signaled to the phone using an alert-info signal. If distinctive ringing is enabled, Cisco Unified CME generates the alert-info for incoming calls from any phone that is not registered in Cisco Unified CME, to the local endpoint. Alert-info from an incoming leg can be relayed to an outgoing leg with the internally generated alert-info taking precedence.

Cisco Unified IP phones use the standard Telcordia Technologies distinctive ring types.

Customized Ringtones

Cisco Unified IP Phones have two default ring types: Chirp1 and Chirp2. Cisco Unified CME also supports customized ringtones using pulse code modulation (PCM) files.

An XML file called RingList.xml specifies the ringtone options available for the default ring on an IP phone registered to Cisco Unified CME. An XML file called DistinctiveRingList.xml specifies the ringtones available on each individual line appearance on an IP phone registered to Cisco Unified CME.

On-Hold Indicator

On-hold indicator is an optional feature that generates a ring burst on idle IP phones that have placed a call on hold. An option is available to generate call-waiting beeps for occupied phones that have placed calls on hold. This feature is disabled by default. For configuration information, see Configure On-Hold Indicator, on page 903.

LED color display for hold state, also known as I-Hold, is supported in Cisco Unified CME 4.0(2) and later versions. The I-Hold feature provides a visual indicator for distinguishing a local hold from a remote hold on shared lines on supported phones, such as the Cisco Unified IP Phone 7931G. This feature requires no additional configuration.

Configure Ringtones

Configure Distinctive Ringing

To set the ring pattern for all incoming calls to a directory number, perform the following steps.

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **ring** {**external** | **internal** | **feature**} [**primary** | **secondary**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 29`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 2333`	Configures a valid extension number for this ephone-dn.
Step 5	**ring** {**external** | **internal** | **feature**} [**primary** | **secondary**] **Example:** `Router(config-ephone-dn)# ring internal`	Designates which ring pattern to be used for all types of incoming calls to this directory number, on all phones on which the directory number appears.
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Configure Customized Ringtones

To create a customized ringtone, perform the following steps.

Before You Begin

Cisco Unified CME 4.0 or a later version.

Step 1 Create a PCM file for each customized ringtone (one ring per file). The PCM files must comply with the following format guidelines.

- Raw PCM (no header)
- 8000 samples per second

- 8 bits per sample
- mLaw compression
- Maximum ring size—16080 samples
- Minimum ring size—240 samples
- Number of samples in the ring must be evenly divisible by 240
- Ring should start and end at the zero crossing

Use an audio editing package that supports these file format requirements to create PCM files for customized phone rings.

Sample ring files are in the ringtone.tar file at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp

Step 2 Edit the RingList.xml and DistinctiveRingList.xml files using a text editor.
The RingList.xml and DistinctiveRingList.xml files contain a list of phone ring types. Each file shows the PCM file used for each ring type and the text that is displayed on the Ring Type menu on a Cisco Unified IP Phone for each ring.

Sample XML files are in the ringtone.tar file at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp

The RingList.xml and DistinctiveRingList.xml files use the following format to specify customized rings:

```
<CiscoIPPhoneRingList>
 <Ring>
  <DisplayName/>
  <FileName/>
 </Ring>
</CiscoIPPhoneRingList>
```

The XML ring files use the following tag definitions:

- Ring files contain two fields, DisplayName and FileName, which are required for each phone ring type. Up to 50 rings can be listed.
- DisplayName defines the name of the customized ring for the associated PCM file that will be displayed on the Ring Type menu of the Cisco Unified IP Phone.
- FileName specifies the name of the PCM file for the customized ring to associate with DisplayName.
- The DisplayName and FileName fields can not exceed 25 characters.

The following sample RingList.xml file defines two phone ring types:

```
<CiscoIPPhoneRingList>
<Ring>
  <DisplayName>Piano1</DisplayName>
  <FileName>Piano1.raw</FileName>
  </Ring>
<Ring>
  <DisplayName>Chime</DisplayName>
  <FileName>Chime.raw</FileName>
  </Ring>
</CiscoIPPhoneRingList>
```

Step 3 Copy the PCM and XML files to system Flash on the Cisco Unified CME router. For example:

```
copy tftp://192.168.1.1/RingList.xml flash:
copy tftp://192.168.1.1/DistinctiveRingList.xml flash:
copy tftp://192.168.1.1/Piano1.raw flash:
copy tftp://192.168.1.1/Chime.raw flash:
```

Step 4 Use the **tftp-server** command to enable access to the files. For example:

```
tftp-server flash:RingList.xml
tftp-server flash:DistinctiveRingList.xml
tftp-server flash:Piano1.raw
tftp-server flash:Chime.raw
```

Step 5 Reboot the IP phones. After reboot, the IP phones download the XML and ringtone files. Select the customized ring by pressing the Settings button followed by the Ring Type menu option on a phone.

Configure On-Hold Indicator

The Call Hold feature is available by default. To define an audible indicator as a reminder that a call is waiting on hold, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **hold-alert** *timeout* {**idle** | **originator** | **shared** | **shared-idle**} [**recurrence** *recurrence-timeout*] [**ring-silent-dn**]
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.

	Command or Action	Purpose
Step 3	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 20`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.
Step 4	**hold-alert** *timeout* {**idle** | **originator** | **shared** | **shared-idle**} [**recurrence** *recurrence-timeout*] [**ring-silent-dn**] **Example:** `Router(config-ephone-dn)# hold-alert 15 idle recurrence 3`	Sets audible alert notification on the Cisco Unified IP phone for alerting the user about on-hold calls. **Note** From the perspective of the originator of the call on hold, the **originator** and **shared** keywords provide the same functionality.
Step 5	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Enable Distinctive Ringing on SIP Phones

To set the ring pattern for distinguishing between external and internal incoming calls, perform the following steps.

Restriction bellcore-dr1 to bellcore-dr5 are the only Telcordia options that are supported for SIP phones.

Before You Begin

Cisco Unified CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **external-ring** {**bellcore-dr1** | **bellcore-dr2** |**bellcore-dr3** | **bellcore-dr4** | **bellcore-dr5**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**external-ring** {**bellcore-dr1** | **bellcore-dr2** |**bellcore-dr3** | **bellcore-dr4** | **bellcore-dr5**} **Example:** `Router(config-register-global)# external-ring bellcore-dr3`	Specifies the type of audible ring sound to be used for external calls • Default—Internal ring sound is used for all incoming calls.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuration Examples for Ringtones

Example for Configuring Distinctive Ringing for Internal Calls

The following example sets distinctive ringing for internal calls on extension 2333.

```
ephone-dn 34
 number 2333
 ring internal
```

Example for Configuring On-Hold Indicator

In the following example, extension 2555 is configured to not forward local calls that are internal to the Cisco Unified CME system. Extension 2222 dials extension 2555. If 2555 is busy, the caller hears a busy tone. If 2555 does not answer, the caller hears ringback. The internal call is not forwarded.

```
ephone-dn 25
 number 2555
```

```
no forward local-calls
call-forward busy 2244
call-forward noan 2244 timeout 45
```

Feature Information for Ringtones

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

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

Table 74: Feature Information for Ringtones

Feature Name	Cisco Unified CME Version	Feature Information
Distinctive Ringing	4.0	Supports ringtone choices for all incoming calls to an individual directory number, for all SCCP phones on which the directory number appears.
	3.4	Generate the alert-info for incoming calls from any phone that is not registered in Cisco Unified CME, to local SIP endpoints.
Customized Ringtones	4.0	Customized Ringtones feature was introduced.
On-Hold Indictor	4.0(2)	Controls LED color display for hold state to provide visual indicator for distinguishing a local hold from a remote hold on shared lines on supported phones, such as the Cisco Unified IP Phone 7931G.
	2.0	Audible on-hold indicator was introduced.
	1.0	Call Hold was introduced.

CHAPTER 33

Single Number Reach

Information About Single Number Reach

Overview of Single Number Reach

The Single Number Reach (SNR) feature allows users to answer incoming calls to their extension on either their desktop IP phone or at a remote destination, such as a mobile phone. Users can pick up active calls on the desktop phone or the remote phone without losing the connection. This enables callers to dial a single number to reach the phone user. Calls that are not answered can be forwarded to voice mail.

Remote destinations may include the following devices:

- Mobile (cellular) phones.
- Smart phones.
- IP phones not belonging to the same Cisco Unified CME router as the desktop phone.
- Home phone numbers in the PSTN. Supported PSTN interfaces include PRI, BRI, SIP, and FXO.

For incoming calls to the SNR extension, Cisco Unified CME rings the desktop IP phone first. If the IP phone does not answer within the configured amount of time, it rings the configured remote number while continuing to ring the IP phone. Unanswered calls are sent to a configured voice-mail number.

The IP phone user has these options for handling calls to the SNR extension:

- Pull back the call from the remote phone—Phone user can manually pull back the call to the SNR extension by pressing the Resume softkey, which disconnects the call from the remote phone.
- Send the call to remote phone—Phone user can send the call to the remote phone by using the Mobility softkey. While connected to the call, the phone user can press the Mobility softkey and select **Send call to mobile**. The call is forwarded to the remote phone.

- Enable or disable Single Number Reach—While the IP phone is in the idle state, the user can toggle the SNR feature on and off by using the Mobility softkey. If the user disables SNR, Cisco Unified CME does not ring the remote number.

IP phone users can modify their own SNR settings directly from the phone by using the menu available with the Services feature button. You must enable the feature on the phone to allow a phone user to access the user interface.

This feature is supported in Cisco Unified CME 7.1 and later versions on SCCP IP phones that support softkeys.

SNR Enhancements

Cisco Unified CME 8.5 supports the following enhancements in the Single Number Reach (SNR) feature:

Hardware Conference

In Cisco Unified CME 8.5, you can send a call to a mobile phone after joining a hardware conference. After joining the hardware conference, all conference callers are blind-transferred to hardware DN. The call character of the ephone changes from incoming call to outgoing call and you are able to send a call to the mobile.

Call Park, Call Pickup, and Call Retrieval

In earlier versions of Cisco Unified CME, Call Park, Call Pickup, and Call Retrieval features were not supported for SNR. Cisco Unified CME 8.5 and later versions allows you to park, pickup, or retrieve an SNR call,

Cisco Unified CME 8.5 enhances the SNR feature to allow you to see the local number on your cell phone instead of the calling party number. You can configure the snr calling number local command under ephone-dn configuration mode to view the caller ID of the SNR phone. For information on configuring SNR calling number local, see Configure Single Number Reach Enhancements on SCCP Phones, on page 915.

Answer Too Soon Timer

On non-FXO ports, you can set an snr answer too soon timer to prevent the calls from rolling to the voice mailbox of your cell phone. When the cell phone rolls to the voice mail within the answer too soon timer range (1 to 5 seconds), the mobile phone call leg is immediately disconnected. You can configure the snr answer too soon command under ephone-dn mode. For more information, see Configure Single Number Reach Enhancements on SCCP Phones, on page 915. The answer-too soon timer is not applicable when sending the call to a mobile.

SNR Phone Stops Ringing After Mobile Phone Answers

When SNR is deployed on non-FXO ports, if cell phone picks up an SNR call, you are connected to the call. The ephone stops ringing further and is placed on hold. You can configure the snr ring-stop command under ephone-dn configuration mode to stop the ephone from ringing and to place the phone on hold. For more information, see Configure Single Number Reach Enhancements on SCCP Phones, on page 915.

Single Number Reach for Cisco Unified SIP IP Phones

Before Cisco Unified CME 9.0, the Single Number Reach (SNR) feature enabled the user to be reached on two numbers: a regular directory number (DN) on the ephone and a public switched telephone network (PSTN) connection (either a PRI/BRI/FXO port or a SIP interface). For incoming calls to the ephone, the Cisco Unified CME called the ephone DN first. When the ephone DN did not answer within a configured time, the Cisco Unified CME called a preconfigured PSTN number while continually calling the ephone DN.

In Cisco Unified CME 9.0 and later versions, the following SNR features are supported for Cisco Unified SIP IP phones:

- Enable and disable the Extension Mobility (EM) feature on a Cisco Unified SIP IP phone—Use the Mobility softkey or PLK as a toggle or use the **mobility** and **no mobility** commands to enable or disable the Mobility feature on a Cisco Unified SIP IP phone.
- Manual pull back of a call on a mobile phone—Use the Resume softkey to manually bring a call back to the SNR DN.
- Send a call to a mobile PSTN phone—Send a call to the mobile PSTN phone using the Mobility softkey while the Cisco Unified SIP IP phone is on a call. Select "**Send call to mobile**" and the call is handed off to the mobile phone.
- Send a call to a mobile phone regardless of whether the SNR phone is the originating or the terminating side—Ensure that the SNR feature is configured in voice register dn or ephone-dn configuration mode to send a call to a mobile phone regardless of whether the SNR phone is the originating or terminating side. Use the Mobility softkey, select "**Send call to mobile**," and the call is handed off to the mobile phone.

For calls from a PSTN, local, or VoIP phone to a Cisco Unified SIP IP phone configured as an SNR phone, the Cisco Unified CME calls the SIP SNR or the mobile phone DN.

When you answer the call on the SIP SNR phone, you can send the call to the PSTN/BRI/PRI/SIP phone.

When you answer the call on the mobile phone, the Resume softkey is displayed on the SIP SNR phone and allows the call to be pulled back to the SIP SNR phone. You can repeatedly pull the call back from the PSTN phone to the SIP SNR phone or from the SIP SNR phone to the PSTN phone.

If the cfwd-noan keyword is configured and both the mobile and SIP SNR phones do not answer, the call is redirected to a preconfigured extension number when the end of a preconfigured time delay is reached.

The following shows how SNR phones configured with Cisco Unified SIP IP phones behave differently from those configured with Cisco Unified SCCP IP phones when sending a call to a mobile:

- For Cisco Unified SCCP IP phones, the Resume softkey is displayed on the SCCP SNR phone as soon as the call is sent to the mobile phone.
- For Cisco Unified SIP IP phones, the Resume softkey is displayed on the SIP SNR phone as soon as the mobile phone answers the call.

Note When the Resume softkey is pressed, the call is returned to the SNR phone.

Cisco Unified CME 9.0 supports the SNR feature in Cisco Unified SIP 7906, 7911, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, 7975, 8961, 9951, and 9971 IP Phones.

Virtual SNR DN for Cisco Unified SCCP IP Phones

A virtual SNR DN is a DN not associated with any registered phone. It can be called, forwarded to a preconfigured mobile phone, or put on an Auto Hold state when the mobile phone answers the call or the time delay is reached. In the Auto Hold state, the DN can either be floating or unregistered. A floating DN is a DN not configured for any phone while an unregistered DN is one associated with phones not registered to a Cisco Unified CME system.

Before Cisco Unified CME 9.0, an SNR DN feature did not launch when the SNR DN was not associated with any registered phone. Although a call could be forwarded to the mobile phone using the **call-forward busy** command, the SNR DN had to be configured under a phone. Users who were assigned floating DNs could not forward calls unless they had a phone assigned to them.

In Cisco Unified CME 9.0 and later versions, an SNR DN is not required to be associated with a registered phone to have the SNR DN feature launched. A call can be made to a virtual SNR DN and the SNR feature can be launched even when the SNR DN is not associated with any phone. A call to a virtual SNR DN can be forwarded to an auto-attendant service when the preconfigured mobile phone is out of service and the voice mail can be retrieved using the telephone or extension number assigned to the voice mailbox.

Although the virtual SNR DN feature is designed for SNR DNs that are not associated with registered phones, this feature also supports virtual SNR DNs that complete phone registration or login and registered DNs that become virtual when all associated registered phones become unregistered.

Configure Single Number Reach

Configure Single Number Reach on SCCP Phones

Restriction

- Each IP phone supports only one SNR directory number.
- SNR feature is not supported for the following:
  - SCCP-controlled analog FXS phones
  - MLPP calls
  - Secure calls
  - Video calls
  - Hunt group directory numbers (voice or ephone)
  - MWI directory numbers
  - Trunk directory numbers
- An overlay set can support only one SNR directory number and that directory number must be the primary directory number.
- Call forward no answer (CFNA), configured with the **call-forward noan** command, is disabled if SNR is configured on the directory number. To forward unanswered calls to voice mail, use the **cfwd-noan** keyword in the **snr** command.
- Call forwarding of unanswered calls, configured with the **cfwd-noan** keyword in the **snr** command, is not supported for PSTN calls from FXO trunks because the calls connect immediately.
- Calls from an internal extension to an extension which is busy, is forwarded to the SNR destination even if **no forward local-calls** is configured under the Directory Number.
- Calls always remain private. If a call is answered on a remote phone, the desktop IP phone can not listen to the call unless it resumes the call.
- U.S. English is the only locale supported for SNR calls.

Before You Begin

- Cisco Unified CME 7.1 or a later version
- Cisco IP Communicator requires version 2.1.4 or later

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number*
5. **mobility**
6. **snr** *e164-number* **delay** *seconds* **timeout** *seconds* [**cfwd-noan** *extension-number*]
7. **snr calling-number local**
8. **exit**
9. **ephone-template** *template-tag*
10. **softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Mobility**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]}
11. **softkeys idle** {[**Cfwdall**] [**ConfList**] [**Dnd**] [**Gpickup**] [**HLog**] [**Join**] [**Login**] [**Mobility**] [**Newcall**] [**Pickup**] [**Redial**] [**RmLstC**]}
12. **exit**
13. **ephone** *phone-tag*
14. **ephone-template** *template-tag*
15. **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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 10`	Enters directory number configuration mode.
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 1001`	Associates an extension number with this directory number. • *number*—String of up to 16 digits that represents an extension or E.164 telephone number.

	Command or Action	Purpose
Step 5	**mobility** **Example:** `Router(config-ephone-dn)# mobility`	Enables the Mobility feature on the directory number.
Step 6	**snr** *e164-number* **delay** *seconds* **timeout** *seconds* [**cfwd-noan** *extension-number*] **Example:** `Router(config-ephone-dn)# snr 4085550133 delay 5 timeout 15 cfwd-noan 2001`	Enables SNR on the extension. • *e164-number*—E.164 telephone number to ring if IP phone extension does not answer. • **delay** *seconds*—Sets the number of seconds that the call rings the IP phone before ringing the remote phone. Range is from 0 to 10. Default: disabled. • **timeout** *seconds*—Sets the number of seconds that the call rings after the configured delay. Call continues to ring for this length of time on the IP phone even if the remote phone answers the call. Range is from 5 to 60. Default: disabled. • **cfwd-noan** *extension-number*—(Optional) Forwards the call to this target number if the phone does not answer after both the **delay** and **timeout** seconds have expired. This is typically the voice-mail number. **Note** The **cfwd-noan** option is not supported for calls from FXO trunks because the calls connect immediately.
Step 7	**snr calling-number local** **Example:** `Router(config-ephone-dn)# snr calling-number local`	(Optional) Replaces the original calling party number with the SNR extension number in the caller ID display of the remote phone. • This command is supported in Cisco Unified CME 8.0 and later versions.
Step 8	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 9	**ephone-template** *template-tag* **Example:** `Router(config)# ephone-template 1`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range is from 1 to 20.
Step 10	**softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Mobility**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]}	Modifies the order and type of softkeys that display on an IP phone during the connected call state. • Pressing the Mobility softkey during the connected call state forwards the call to the PSTN number defined in Step 6.

	Command or Action	Purpose
	Example: `Router(config-ephone-template)# softkeys connected endcall hold livercd mobility`	
Step 11	**softkeys idle** {[**Cfwdall**] [**ConfList**] [**Dnd**] [**Gpickup**] [**HLog**] [**Join**] [**Login**] [**Mobility**] [**Newcall**] [**Pickup**] [**Redial**] [**RmLstC**]} **Example:** `Router(config-ephone-template)# softkeys idle dnd gpickup pickup mobility`	Modifies the order and type of softkeys that display on an IP phone during the idle call state. • Pressing the Mobility softkey during the idle call state enables the SNR feature. This key is a toggle; pressing it a second time disables SNR.
Step 12	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 13	**ephone** *phone-tag* **Example:** `Router(config)# ephone 21`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 14	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 1`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the ephone template that you created in Step 12.
Step 15	**end** **Example:** `Router(config-ephone-template)# end`	Exits configuration mode.

The following example shows extension 1001 is enabled for SNR on IP phone 21. After a call rings at this number for 5 seconds, the call also rings at the remote number 4085550133. The call continues ringing on both phones for 15 seconds. If the call is not answered after a total of 20 seconds, the call no longer rings and it is forwarded to the voice-mail number 2001.

```
ephone-template  1
 softkeys idle  Dnd Gpickup Pickup Mobility
 softkeys connected  Endcall Hold LiveRcd Mobility
!
ephone-dn 10
 number 1001
 mobility
 snr 4085550133 delay 5 timeout 15 cfwd-noan 2001
 snr calling-number local
!
!
ephone  21
 mac-address 02EA.EAEA.0001
```

```
ephone-template 1
button  1:10
```

Configure Single Number Reach Enhancements on SCCP Phones

Restriction

- Software Conference— After a software conference is initiated and committed on an ephone, you cannot send the call to a mobile phone. You can only enable or disable mobility after software conference is committed.
- SNR Call Pickup on FXO port— For a call routed through FXO port to the PSTN, the call is signaled as "connected" as soon as FXO port is seized outbound. The mobile phone is on FXO interface and the call (session) is in active state as soon as FXO is in connect state. The ephone will be in ringing state but you can not pick up the ephone call.
- Music on hold (MOH) is not supported if the SNR call originates from the line side. MOH is supported on an SNR call if the call originates from the trunk side.

Before You Begin

Cisco Unified CME 8.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **mobility**
6. **snr calling number local**
7. **snr answer too soon** *time*
8. **snr ring-stop**
9. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 10`	Enters directory number configuration mode.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 1001`	Associates an extension number with this directory number. • *number*—String of up to 16 digits that represents an extension or E.164 telephone number.
Step 5	**mobility** **Example:** `Router(config-ephone-dn)# mobility`	Enables the Mobility feature on the directory number.
Step 6	**snr calling number local** **Example:** `Router(config-ephone-dn)#snr calling-number local`	Displays local number as calling number on your SNR mobile phone.
Step 7	**snr answer too soon** *time* **Example:** `Router(config-ephone-dn)#snr answer-too-soon 4`	Enables a timer for answering the call on SNR mobile phone. • time—Time, in seconds. Range is from 1 to 5.
Step 8	**snr ring-stop** **Example:** `Router(config-ephone-dn)#snr ring-stop`	Allows you to stop the IP phone from ringing after the SNR call is answered on a mobile phone.
Step 9	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.

The following example shows SNR enhancements configured for ephone-dn 10:

```
Router#show running config
!
!
telephony-service
 sdspfarm units 1
 sdspfarm tag 1 confprof1
 conference hardware
 max-ephones 262
 max-dn 720
 ip source-address 172.19.153.114 port 2000
 service phone thumbButton PTTH6
```

```
 load 7906 SCCP11.8-5-3S.loads
 load 7911 SCCP11.8-5-3S.loads
!
ephone-template  6
 feature-button 1 Hold
!
!
ephone-dn  10
 mobility
```
snr calling-number local
snr ring-stop
snr answer-too-soon 4

Configure Single Number Reach on SIP Phones

Restriction

- Hardware Conferencing and Privacy on Hold for Cisco Unified SIP IP phones are not supported.
- Mixed shared lines between Cisco Unified SIP and SCCP IP phones are not supported.
- Subscribe and Notify modes for SIP shared lines are not supported.
- Incoming calls from the H323 IP trunk are not supported.
- Media flow around for SIP-SIP trunk calls is not supported.
- SIP SNR phones that initiate software conferencing are unable to send or receive calls to or from mobile phones because the Cisco Unified SIP IP phones are put on hold after a software conference is committed.

Before You Begin

Cisco Unified CME 9.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **softkeys idle** {[**Cfwdall**] [**DND**] [**Gpickup**] [**Newcall**] [**Pickup**] [**Redial**]}
5. **softkeys connected** {[**Confrn**] [**Endcall**] [**Hold**] [**Park**] [**Trnsfer**] [**iDivert**]}
6. **exit**
7. **voice register pool** *pool-tag*
8. **session-transport** {**tcp**}
9. **exit**
10. **voice register dn** *dn-tag*
11. **number** *number*
12. **name** *name*
13. **mobility**
14. **snr calling-number local**
15. **snr** *e164-number* **delay** *seconds* **timeout** *seconds* [**cfwd-noan** *extension-number*]
16. **snr ring-stop**
17. **snr answer-too-soon** *time*
18. **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 register template** *template-tag* **Example:** `Router(config)# voice register template 1`	Enters voice register template configuration mode. • *template-tag*—identifier for the template being created. Range: 1 to 10.
Step 4	**softkeys idle** {[**Cfwdall**] [**DND**] [**Gpickup**] [**Newcall**] [**Pickup**] [**Redial**]} **Example:** `Router(config-register-temp)# softkeys idle Redial Cfwdall`	Modifies the display of softkeys on Cisco Unified SIP IP phones during the idle call state. • **Cfwdall**—(Optional) Softkey for "call forward all." Forwards all calls. • **DND**—(Optional) Softkey that enables the Do-Not-Disturb feature.

	Command or Action	Purpose
		• **Gpickup**—(Optional) Softkey that allows a user to pickup a call that is ringing on another phone. • **Newcall**—(Optional) Softkey that opens a line on a speakerphone to place a new call. • **Pickup**—(Optional) Softkey that allows a user to pickup a call that is ringing on another phone that is a member of the same pickup group. • **Redial**—(Optional) Softkey that redials the last number dialed.
Step 5	**softkeys connected** {[**Confrn**] [**Endcall**] [**Hold**] [**Park**] [**Trnsfer**] [**iDivert**]} **Example:** `Router(config-register-temp)# softkeys connected Confrn Hold Endcall`	Modifies the display of softkeys on Cisco Unified SIP IP phones during the connected call state. • **Confrn**—(Optional) Softkey that connects callers to a conference call. • **Endcall**—(Optional) Softkey that ends the current call. • **Hold**—(Optional) Softkey that places an active call on hold and resumes the call. • **Park**—(Optional) Softkey that places an active call on hold, so it can be retrieved from another phone in the system. • **Trnsfer**—(Optional) Softkey that transfers active calls to another extension. • **iDivert**—(Optional) Softkey that immediately diverts a call to a voice-messaging system.
Step 6	**exit** **Example:** `Router(config-register-temp)# exit`	Exits voice register template configuration mode.
Step 7	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 10`	Enters voice register pool configuration mode. • *pool-tag*—Unique number assigned to the pool. Range: 1 to 100. **Note** For Cisco Unified CME systems, the upper limit for this argument is defined by the **max-pool** command.
Step 8	**session-transport** {**tcp**} **Example:** `Router(config-register-pool)# session-transport tcp`	Specifies the transport layer protocol that a Cisco Unified SIP IP phone uses to connect to Cisco Unified CME. • **tcp**—Transmission Control Protocol (TCP) is used.
Step 9	**exit** **Example:** `Router(config-register-pool)# exit`	Exits voice register pool configuration mode.

	Command or Action	Purpose
Step 10	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 3`	Enters voice register dn configuration mode. • *dn-tag*—Unique sequence number that identifies a particular directory number during configuration tasks. Range is 1 to 150 or the maximum defined by the **max-dn** command.
Step 11	**number** *number* **Example:** `Router(config-register-dn)# number 1004`	Associates a telephone or extension number with a Cisco Unified SIP IP phone in a Cisco Unified CME system. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally, the string is composed of digits, but the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number.
Step 12	**name** *name* **Example:** `Router(config-register-dn)# name John Smith`	Associates a name with a directory number in Cisco Unified CME. • *name*—Name of the person associated with a given extension. Name must follow the order specified in the **directory** (telephony-service) command, either **first-name-first** or **last-name-first**.
Step 13	**mobility** **Example:** `Router(config-register-dn)# mobility`	Enables the Mobility feature on an extension of a Cisco Unified SIP IP phone.
Step 14	**snr calling-number local** **Example:** `Router(config-register-dn)# snr calling-number local`	Replaces the calling party number displayed on the configured mobile phone with the local SNR number.
Step 15	**snr** *e164-number* **delay** *seconds* **timeout** *seconds* [**cfwd-noan** *extension-number*] **Example:** `Router(config-register-dn)# snr 9900 delay 1 timeout 10`	Enables the SNR feature on an extension of a Cisco Unified SIP IP phone. • *e164-number*—E.164 telephone number to call when the Cisco Unified SIP IP phone extension does not answer. • **delay** *seconds*—Sets the number of seconds that the Cisco Unified SIP IP phone rings when called. When the time delay is reached, the call is transferred to the PSTN phone and the SNR directory number. Range: 0 to 30. Default: 5. • **timeout** *seconds*—Sets the number of seconds that the Cisco Unified SIP IP phone rings after the configured time delay. When the timeout value is reached, no call is displayed on the phone. You have to use the Resume softkey to pull back or the Mobility softkey to send the call to a mobile phone. Range: 30 to 60. Default: 60. **Note** When the default is enabled, the Cisco Unified SIP IP phone continues to ring for 60 seconds even if the remote phone answers the call.

	Command or Action	Purpose
		• **cfwd-noan** *extension-number*—(Optional) Forwards the call to the extension number when the phone does not answer after both the time delay and timeout values are reached. The extension number is typically the voice mail number. **Note** This option is not supported for calls from FXO trunks because the calls connect immediately.
Step 16	**snr ring-stop** **Example:** `Router(config-register-dn)# snr ring-stop`	Ends the ringing on a Cisco Unified SIP IP phone after the SNR call is answered on the configured mobile phone.
Step 17	**snr answer-too-soon** *time* **Example:** `Router(config-register-dn)# snr answer-too-soon 2`	Sets the time in which SNR calls are prevented from being diverted to the voice mailbox of a mobile phone. • *time*—Time, in seconds. Range: 1 to 5.
Step 18	**end** **Example:** `Router(config-register-dn)# end`	Exits voice register dn configuration mode and enters privileged EXEC mode.

Configure a Virtual SNR DN on SCCP Phones

Restriction

- Virtual SNR DN only supports Cisco Unified SCCP IP phone DNs.
- Virtual SNR DN provides no mid-call support.

  Mid-calls are either of the following:

  - Calls that arrive before the DN is associated with a registered phone and is still present after the DN is associated with the phone.
  - Calls that arrive for a registered DN that changes state from registered to virtual and back to registered.

- Mid-calls cannot be pulled back, answered, or terminated from the phone associated with the DN.
- State of the virtual DN transitions from ringing to hold or remains on hold as a registered DN.

Before You Begin

Cisco Unified CME 9.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number*
5. **mobility**
6. **snr mode** [**virtual**]
7. **snr** *e164-number* **delay** *seconds* **timeout** *seconds* [**cfwd-noan** *extension-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	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 10`	Enters ephone-dn configuration mode to configure a directory number for an IP phone line. • *dn-tag*—Unique number that identifies an ephone-dn during configuration tasks. Range is 1 to the number set by the **max-dn** command.
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 1001`	Associates a telephone or extension number with this ephone-dn. • *number*—String of up to 16 characters that represents an E.164 telephone number. Normally, the string is composed of digits, but the string may contain alphabetic characters when the number is dialed only by the router, as with an intercom number.
Step 5	**mobility** **Example:** `Router(config-ephone-dn)# mobility`	Enables the Mobility feature on an extension of a Cisco Unified SCCP IP phone.
Step 6	**snr mode** [**virtual**] **Example:** `Router(config-ephone-dn)# snr mode virtual`	Sets the mode for the SNR directory number. • **virtual—**Enables the virtual mode for an SNR DN when it is unregistered or floating.

	Command or Action	Purpose
Step 7	**snr** *e164-number* **delay** *seconds* **timeout** *seconds* [**cfwd-noan** *extension-number*] **Example:** `Router(config-ephone-dn)# snr 408550133 delay 5 timeout 15 cfwd-noan 2001`	Enables the Single Number Reach feature on the extension of a Cisco Unified SCCP IP phone. • *e164-number*—E.164 telephone number to ring if IP phone extension does not answer. • **delay** *seconds*—Sets the number of seconds that the call rings the IP phone before ringing the remote phone. Range: 0 to 10. Default: disabled. • **timeout** *seconds*—Sets the number of seconds that the call rings after the configured delay. Call continues to ring for this length of time on the IP phone even if the remote phone answers the call. Range: 5 to 60. Default: disabled. • **cfwd-noan** *extension-number*—(Optional) Forwards the call to this target number if the phone does not answer after both the delay and timeout seconds have expired. This is typically the voice mail number.
Step 8	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.

Feature Information for Single Number Reach

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

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

Table 75: Feature Information for Single Number Reach

Feature Name	Cisco Unified CME Version	Modification
Single Number Reach for Cisco Unified SIP IP Phones	9.0	Supports the following SNR features for Cisco Unified SIP IP phones: • Enable and disable the EM feature. • Manual pull back of a call on a mobile phone. • Send a call to a mobile PSTN phone. • Send a call to a mobile phone regardless of whether the SNR phone is the originating or the terminating side.
Virtual SNR DN for Cisco Unified SCCP IP Phones		Allows a call to be made to a virtual SNR DN and allows the SNR feature to be launched even when the SNR DN is not associated with any phone.
SNR Enhancements	8.5	Added support for the following SNR enhancements: • Hardware Conference • Call Park, Call Pickup, and Call Retrieval • Answer Too Soon Timer • SNR Phone Stops Ringing After Mobile Phone Answers
Calling Number Local	8.0	Added the **snr calling-number local** command to replace the calling party number with the SNR extension in the caller ID display.
Single Number Reach	7.1	Introduced the SNR feature.

CHAPTER 34

Customize Softkeys

Information About Softkeys

Softkeys on IP Phones

You can customize the display and order of softkeys that appear during various call states on individual IP phones. Softkeys that are appropriate in each call state are displayed by default. Using phone templates, you can delete softkeys that would normally appear or change the order in which the softkeys appear. For example, you might want to display the **CFwdAll** and **Confrn** softkeys on a manager's phone and remove these softkeys from a receptionist's phone.

You can modify softkeys for the following call states:

- Alerting—When the remote point is being notified of an incoming call and the status of the remote point is being relayed to the caller as either ringback or busy.
- Connected—When the connection to a remote point is established.
- Hold—When a connected party is still connected but there is temporarily no voice connection.
- Idle—Before a call is made and after a call is completed.
- Seized—When a caller is attempting a call but has not yet been connected.
- Remote-in-Use—When another phone is connected to a call on an octo-line directory number shared by this phone (Cisco Unified CME 4.3 or a later version).
- Ringing—After a call is received and before the call is connected (Cisco Unified CME 4.2 or a later version).

Not all softkeys are available in all call states. Use the CLI help to see the available softkeys for each call state. The softkeys are as follows:

- Acct—Short for "account code." Provides access to configured accounts.
- Answer—Picks up incoming call.
- Barge—Allows a user to join (barge) a call on a SIP shared line (Cisco Unified CME 7.1 or a later version).
- Callback—Requests callback notification when a busy called line becomes free.
- CBarge—Barges (joins) a call on a shared octo-line directory number (Cisco Unified CME 4.3 or a later version).
- CFwdALL—Short for "call forward all." Forwards all calls.
- ConfList—Lists all parties in a conference (Cisco Unified CME 4.1 or a later version). Press **Update** softkey to update the list of parties in the conference, for instance, to verify that a party has been removed from the conference. Press **Remove** softkey to remove the appropriate parties.
- Confrn—Short for "conference." Connects callers to a conference call.
- Details—Lists all the participants in a conference. This softkey is supported only on Cisco 7800 Series IP Phones. Press **Update** to update the list of parties in the conference. Press **Remove** softkey to remove the appropriate parties. The suboption **Remove** is available to the conference creator and phones that have **conference admin** configured.
- DND—Short for "do not disturb." Enables the do-not-disturb features.
- EndCall—Ends the current call.
- GPickUp—Short for "group call pickup." Selectively picks up calls coming into a phone number that is a member of a pickup group.
- Flash—Short for "hookflash." Provides hookflash functionality for public switched telephone network (PSTN) services on calls connected to the PSTN via a foreign exchange office (FXO) port.
- HLog—Places the phone of an ephone-hunt group agent into the not-ready status or, if the phone is in the not-ready status, places the phone into the ready status.
- Hold—Places an active call on hold and resumes the call.
- iDivert—Immediately diverts a call to a voice messaging system (Cisco Unified CME 8.5 or a later version)
- Join—Joins an established call to a conference (Cisco Unified CME 4.1 or a later version).
- LiveRcd—Starts the recording of a call (Cisco Unified CME 4.3 or a later version).
- Login—Provides personal identification number (PIN) access to restricted phone features.
- MeetMe—Initiates a meet-me conference (Cisco Unified CME 4.1 or a later version).
- Mobility—Forwards a call to the PSTN number defined by the Single Number Reach (SNR) feature (Cisco Unified CME 7.1 or a later version).
- NewCall—Opens a line on a speakerphone to place a new call.
- Park—Places an active call on hold so it can be retrieved from another phone in the system.
- PickUp—Selectively picks up calls coming into another extension.

- Redial—Redials the last number dialed.
- Resume—Connects to the call on hold.
- RmLstC—Removes the last party added to a conference. This softkey only works for the conference creator (Cisco Unified CME 4.1 or a later version).
- Select—Selects a call or a conference on which to take action (Cisco Unified CME 4.1 or a later version).
- Show detail—Lists all the participants in a conference. This softkey is supported only on Cisco 8800 Series IP Phones. Press **Update** to update the list of parties in the conference. Press **Remove** softkey to remove the appropriate parties. The suboption **Remove** is available to the conference creator and phones that have **conference admin** configured.
- Trnsfer—Short for "call transfer." Transfers an active call to another extension.
- TrnsfVM—Transfers a call to a voice-mail extension number (Cisco Unified CME 4.3 or a later version).

You change the softkey order by defining a phone template and applying the template to one or more phones. You can create up to 20 phone templates for SCCP phones and 10 templates for SIP phones. Only one template can be applied to a phone. If you apply a second phone template to a phone that already has a template applied to it, the second template overwrites the first phone template information. The new information takes effect only after you generate a new configuration file and restart the phone; otherwise, the previously configured template remains in effect.

In Cisco Unified CME 4.1, customizing the softkey display for IP phones running SIP is supported only for the Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.

For configuration information, see Customize Softkeys, on page 925.

Account Code Entry

The Cisco Unified IP Phones 7940 and 7940G and the Cisco Unified IP Phones 7960 and 7960G allow phone users to enter account codes during call setup or when connected to an active call using the **Acct** softkey. Account codes are inserted into call detail records (CDRs) on the Cisco Unified CME router for later interpretation by billing software.

An account code is visible in the output of the **show call active** command and the **show call history** command for telephony call legs and is supported by the CISCO-VOICE-DIAL-CONTROL-MIB. The account code also appears in the "account-code" RADIUS vendor-specific attribute (VSA) for voice authentication, authorization, and accounting (AAA).

To enter an account code during call setup or when in a connected state, press the **Acct** softkey, enter the account code using the phone keypad, then press the # key to notify Cisco Unified CME that the last digit of the code has been entered. The account code digits are processed upon receipt of the # and appear in the show output after processing.

No configuration is required for this feature.

Note If the # key is not pressed, each account code digit is processed only after a timer expires. The timer is 30 seconds for the first digit entered, then *n* seconds for each subsequent digit, where *n* equals the number of seconds configured with the **timeouts interdigit (telephony-service)** command. The default value for the interdigit timeout is 10 seconds. The account code digits do not appear in the **show** command output until after being processed.

Hookflash Softkey

The Flash softkey provides hookflash functionality for calls made on IP phones that use FXO lines attached to the Cisco Unified CME system. Certain PSTN services, such as three-way calling and call waiting, require hookflash intervention from a phone user.

When a Flash softkey is enabled on an IP phone, it can provide hookflash functionality during all calls except for local IP-phone-to-IP-phone calls. Hookflash-controlled services can be activated only if they are supported by the PSTN connection that is involved in the call. The availability of the Flash softkey does not guarantee that hookflash-based services are accessible to the phone user.

For configuration information, see Enable Flash Softkey, on page 945 .

Feature Blocking

In Cisco Unified CME 4.0 and later versions, individual softkey features can be blocked on one or more phones. You specify the features that you want blocked by adding the **features blocked** command to an ephone template. The template is then applied under ephone configuration mode to one or more ephones.

If a feature is blocked using the **features blocked** command, the softkey is not removed but it does not function. For configuration information, see Configure Feature Blocking, on page 947.

To remove a softkey display, use the appropriate **no softkeys** command. See Modify Softkey Display on SCCP Phone, on page 938.

Feature Policy Softkey Control

Cisco Unified CME 8.5 allows you to control the display of softkeys on the Cisco Unified SIP IP Phones 8961, 9951, and 9971 using the Feature Policy template. The Feature Policy template allows you to enable and disable a list of feature softkeys on Cisco Unified SIP IP Phones 8961, 9951, and 9971. Table 76: Feature IDs and Default State of the Controllable Features, on page 928 lists the controllable feature softkeys with specific feature IDs and their default state on Cisco Unified SIP IP Phones 8961, 9951, and 9971.

Table 76: Feature IDs and Default State of the Controllable Features

Feature ID	Feature Name	Description	Default State on CME
1	ForwardAll	Forward all calls	Enabled
2	Park	Parks a call	Enabled
3	iDivert	Divert to Voicemail	Enabled
4	ConfList	Conference List	Disabled
5	SpeedDial	Abbreviated Dial	Disabled
6	Callback	Call back	Disabled
7	Redial	Redial a call	Enabled

Feature ID	Feature Name	Description	Default State on CME
8	Barge	Barge into a call	Enabled

Cisco Unified CME uses the existing **softkey** command under voice register template configuration mode to control the controllable feature softkeys on phones. Cisco Unified CME generates a `featurePolicy<x>.xml` file for each `voice register template <x>` configured. The list of controllable softkey configurations are specified in the `featurePolicy<x>.xml` file. Phones need to reboot or reset to download the Feature Policy template file. For Cisco IP phones that do not have a Feature Policy template assigned to them, you can use the default Feature Policy template file (`featurePolicyDefault.xml` file).

Immediate Divert for SIP IP Phones

The immediate divert (iDivert) feature allows you to immediately divert a call to a voice messaging system. You can divert a call by pressing the **iDivert** softkey on Cisco Unified SIP IP phones with voice messaging systems (Cisco Unity Express or Cisco Unity), such as 7940, 7040G, 7960 G, 7945, 7965, 7975, 8961, 9951, and 9971. When the call is diverted, the line becomes available to place or receive new calls.

The call that is diverted using the iDivert feature can be in ringing, active, or hold state. When the call diversion is successful, the caller receives greetings from the voice messaging system.

Callers can only divert the calls to their own voice mailbox. But calls on the receiver side can be diverted either to the voice mailbox of the caller who invoked the iDivert feature (last redirected party) or to the voice mailbox of the original called party.

The iDivert softkey is added to the phones when they register with Cisco Unified CME using `softkeyxxxx.xml` file. Cisco Unified CME generates the `softkeyxxxx.xml` file when the **create profile** command is executed in voice register global configuration mode. You can disable or change the position of the iDivert softkey on the phone's display using the **softkey** command. For more information, see Configure Immediate Divert (iDivert) Softkey on SIP Phone, on page 949.

Programmable Line Keys (PLK)

The Programmable Line Key (PLK) feature allows you to program feature buttons or services URL buttons on line key buttons. You can configure line keys with line buttons, speed dials, BLF speed dials, feature buttons, and URL buttons.

Note When button layout is not specified, buttons are assigned to the phone lines in the following order: line, speed-dial, blf-speed-dial, feature, and services URL buttons.

You can program a line key to function as a services URL button on your Cisco Unified phone using the **url-button** command (see Configure Service URL Line Key Button on SCCP Phone, on page 951 and Configure Service URL Line Key Button on SIP Phone, on page 953). Similarly, you can program a line key on your Cisco IP phone to function as a feature button using the **feature-button** command (see Configure Feature Buttons on SCCP Phone Line Key, on page 955 and Configure Feature Buttons on SIP Phone Line Key, on page 957 for more information).

You can also program line keys to function as feature buttons using the user-profile in phones that have Extension Mobility (EM) enabled on them. For configuring line keys to function as feature buttons on EM phones, see Cisco Unified IP Phone documentation.

Table 77: PLK Feature Availability on Different Phone Models, on page 930 lists the softkeys supported as PLKs on various Cisco Unified IP Phone models.

Table 77: PLK Feature Availability on Different Phone Models

Softkeys Supported as Programmable Line Keys (PLK)	7914, 7915, 7916 SCCP Phones	7931 Phone	6900 Series SCCP Phones	7942, 7962, 7965, 7975 SIP Phones	8961, 9951, and 9971 SIP Phones
Acct	Supported	Supported	Supported	Not Supported	Not Supported
Call Back	Supported	Supported	Supported	Not Supported	Not Supported
Conference	Supported	Supported	Not Supported [9]	Supported	Not Supported
Conference List	Supported	Supported	Supported	Not Supported	Not Supported
Customized URL	Supported	Supported	Supported	Supported	Not Supported
Do Not Disturb	Supported	Supported	Supported	Supported	Supported
End Call	Supported	Supported	Supported	Supported	Not Supported
Extension Mobility	Supported	Supported	Supported	Not Supported	Not Supported
Forward All	Supported	Supported	Supported	Supported	Not Supported
GPickUp	Supported	Supported	Supported	Supported	Supported
Hold	Supported	Not Supported [1]	Not Supported [1]	Supported	Not Supported
Hook Flash	Supported	Supported	Supported	Not Supported	Not Supported
Hunt Group	Supported	Supported	Supported	Not Supported	Not Supported
Live Record	Supported	Supported	Supported	Not Supported	Not Supported
Login	Supported	Supported	Supported	Not Supported	Not Supported
Meet Me	Supported	Supported	Supported	Not Supported	Not Supported
Mobility	Supported	Supported	Supported	Not Supported	Not Supported
MyPhoneApps	Supported	Supported	Supported	Not Supported	Not Supported

Softkeys Supported as Programmable Line Keys (PLK)	7914, 7915, 7916 SCCP Phones	7931 Phone	6900 Series SCCP Phones	7942, 7962, 7965, 7975 SIP Phones	8961, 9951, and 9971 SIP Phones
New Call	Supported	Supported	Supported	Supported	Not Supported
Night Service	Supported	Supported	Supported	Not Supported	Not Supported
Park	Supported	Supported	Supported	Supported	Supported
Personal Speed Dial	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
PickUp	Supported	Supported	Supported	Supported	Supported
Privacy	Supported	Supported	Supported	Supported	Supported
Redial	Supported	Not Supported [1]	Supported	Supported	Supported
Remove Last Participant	Supported	Supported	Supported	Not Supported	Not Supported
Reset Phone	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Services URL	Not Supported [1]	Not Supported [10]	Not Supported [11]	Not Supported	Not Supported
Speed Dial Buttons	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Single Number Reach	Supported	Supported	Supported	Not Supported	Not Supported
Transfer	Supported	Not Supported [1]	Not Supported [1]	Supported	Not Supported
Transfer to VM	Supported	Supported	Supported	Not Supported	Not Supported

9 This feature is available through a hard button.
10 This feature is available through the application button.
11 This feature is available through the Set button.

Table 78: PLK Feature Availability on the Cisco Unified 6945, 8941, and 8945 SCCP IP Phones in Cisco Unified CME 8.8, on page 932 lists the PLK features available on the Cisco Unified 6945, 8941, and 8945 SCCP IP Phones in Cisco Unified CME 8.8.

Table 78: PLK Feature Availability on the Cisco Unified 6945, 8941, and 8945 SCCP IP Phones in Cisco Unified CME 8.8

Softkeys Supported as Programmable Line Keys	Cisco Unified 6945, 8941, and 8945 SCCP IP Phones
Acct	Supported
Call Back	Supported
Cancel Call Waiting	Supported
Conference List	Supported
Customized URL	Supported
Do Not Disturb	Supported
End Call	Supported
Extension Mobility	Supported
Forward All	Supported
Group Pickup	Supported
Hook Flash	Supported
Hunt Group Login (HLog)	Supported
Live Record	Supported
Login	Supported
Meet Me	Supported
Mobility	Supported
My Phone Apps	Supported
New Call	Supported
Night Service	Supported
Park	Supported
Personal Speed Dial	Not Supported
Pickup	Supported
Privacy	Supported
Redial	Supported

Softkeys Supported as Programmable Line Keys	Cisco Unified 6945, 8941, and 8945 SCCP IP Phones
Remove Last Participant	Supported
Reset Phone	Not Supported
Services URL	Not Supported
Speed Dial Buttons	Supported
Single Number Reach	Supported
Transfer to VM	Supported

Table 79: PLK Feature Availability on the Cisco Unified 6911, 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones in Cisco Unified CME 9.0, on page 933 lists the PLK features available on the Cisco Unified 6911, 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones in Cisco Unified CME 9.0.

Table 79: PLK Feature Availability on the Cisco Unified 6911, 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones in Cisco Unified CME 9.0

Softkeys Supported as Programmable Line Keys	Cisco Unified 6911 SIP IP Phones	Cisco Unified 6921, 6941, 6945, and 6961 SIP IP Phones	Cisco Unified 8941 and 8945 SIP IP Phone
Acct	Not Supported	Not Supported	Not Supported
Call Back	Not Supported	Not Supported	Not Supported
Conference	Not Supported	Not Applicable[12]	Not Applicable[1]
Conference List	Not Supported	Supported	Supported
Customized URL	Not Supported	Supported	Not Supported
Do Not Disturb	Not Supported	Supported	Supported
End Call	Not Supported	Supported	Supported
Extension Mobility	Not Supported	Supported	Supported
Forward All	Supported	Supported	Supported
Group Pickup	Supported	Supported	Supported
Hold	Supported	Supported	Supported
Hook Flash	Not Supported	Not Supported	Not Supported

Softkeys Supported as Programmable Line Keys	Cisco Unified 6911 SIP IP Phones	Cisco Unified 6921, 6941, 6945, and 6961 SIP IP Phones	Cisco Unified 8941 and 8945 SIP IP Phone
Hunt Group	Not Supported	Not Supported	Not Supported
Live Record	Not Supported	Not Supported	Not Supported
Login	Not Supported	Not Supported	Not Supported
Meet Me	Supported	Supported	Supported
Mobility	Not Supported	Supported	Supported
My Phone Apps	Not Supported	Supported	Supported
New Call	Not Supported	Supported	Supported
Night Service	Not Supported	Not Supported	Not Supported
Park	Not Supported	Supported	Supported
Personal Speed Dial	Not Supported	Not Supported	Not Supported
Pickup	Supported	Supported	Supported
Privacy	Supported	Supported	Supported
Redial	Supported	Supported	Supported
Remove Last Participant	Not Supported	Not Supported	Not Supported
Reset Phone	Not Supported	Not Supported	Not Supported
Services URL	Not Supported	Not Supported	Not Supported
Single Number Reach	Not Supported	Supported	Not Supported
Speed Dial	Supported	Supported	Supported
Transfer	Not Supported	Not Applicable[13]	Not Applicable[2]
Transfer to VM	Not Supported	Not Supported	Not Supported

12 These phones are equipped with “conference” hard keys.
13 These phones are equipped with “transfer” hard keys.

Cisco Unified IP Phones 7902, 7905, 7906, 7910, 7911, 7912, 7935, 7936, 7937, 7940, 7960, and 7985 do not support the PLK feature. The services URL button is not supported on the following Cisco Unified IP phones: 7920, 7921, 7925 (supports DnD and Privacy only), 3911, and 3951.

Table 80: PLK Feature Availability on the Cisco Unified 7800, 8800 Series SIP IP Phones from Cisco Unified CME 11.0 Onwards, on page 935 lists the PLK features available on the Cisco Unified 7800 and 8800 series SIP IP Phones from Cisco Unified CME Release 11.0 onwards. As part of Unified CME Release 11.7, new phone support for Cisco IP Phones 8821, 8845, 8865 was introduced. With this addition, Unified CME supports all phone models in Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series.

Table 80: PLK Feature Availability on the Cisco Unified 7800, 8800 Series SIP IP Phones from Cisco Unified CME 11.0 Onwards

Softkeys Supported as Programmable Line Keys	Cisco Unified 7800 Series SIP IP Phones	Cisco Unified 8800 Series SIP IP Phones
Acct	Not Supported	Not Supported
Call Back	Not Supported	Not Supported
Conference	Not Supported	Not Supported
Conference List	Supported	Supported
Customized URL	Not Supported	Not Supported
Do Not Disturb	Supported	Supported
End Call	Supported	Supported
Extension Mobility	Supported	Supported
Forward All	Supported	Supported
Group Pickup	Supported	Supported
Hold	Supported	Supported
Hook Flash	Not Supported	Not Supported
HLog (From Unified CME Release 11.6 onwards)	Supported	Supported
Live Record	Not Supported	Not Supported
Login	Not Supported	Not Supported
Meet Me	Supported	Supported
Mobility	Supported	Supported
My Phone Apps	Supported	Supported
New Call	Supported	Supported

Softkeys Supported as Programmable Line Keys	Cisco Unified 7800 Series SIP IP Phones	Cisco Unified 8800 Series SIP IP Phones
Park	Supported	Supported
Personal Speed Dial	Not Supported	Not Supported
Pickup	Supported	Supported
Privacy	Supported	Supported
Redial	Supported	Supported
Remove Last Participant	Not Supported	Not Supported
Reset Phone	Not Supported	Not Supported
Services URL	Not Supported	Not Supported
Single Number Reach	Not Supported	Not Supported
Speed Dial	Supported	Supported
Transfer	Not Supported	Not Supported
Transfer to VM	Not Supported	Not Supported

Table 81: LED Behavior, on page 936 lists the feature buttons and their corresponding LED behavior. Only features with radio icons will indicate their state via LED.

Table 81: LED Behavior

Feature	Label/Tagged ID	Label/Extended Tagged ID	Icon	LED Behavior
Redial	Redial/SkRedialTag 0x01	—	Default	—
Hold	Hold/SkHoldTag 0x03	—	Hold	—
Transfer	Transfer/SkTrnsferTag 0x04	—	Transfer	—
Forward All		Forward All/0x2D	Default	—
MeetMe	MeetMe/ SkMeetMeConfrn Tag 0x10	—	Default	—

Feature	Label/Tagged ID	Label/Extended Tagged ID	Icon	LED Behavior
Conference	Conference/SkConfrmTag 0x34	—	Conference	—
Park	Park/SkParkTag 0x0E	—	Default	—
PickUp	PickUp/SkCallPickUpTag 0x11	—	Default	—
GPickUp	—	Group PickUp/0x2F	Default	—
Mobility	—	Mobility/0x2B	Mobility	—
Do Not Disturb	—	Do Not Disturb/0x0f	Radio Button	On—active Off—inactive
Conference List	—	Conference List/0x34	Default	—
Remove Last Participant	—	Remove Last Participant/0x30	Default	—
CallBack	CallBack/SkCallBackTag 0x41	—	Default	—
New Call	NewCall/SkNewCallTag 0x02	—	Default	—
End Call	—	End Call/0x33	Default	—
Cancel Call Waiting	CW Off	—	Default	—
HLog	—	Hunt Group/0x36	Default	On—hlog in Off—hlog out Blink—call in queue at Hlogout state
Privacy	Private/ SkPrivacy 0x36	—	Radio Button	On—active Off—inactive
Acct	Acct/ TAGS_ACCT_ 40 TAGS_Acct[]	—	Default	—

Feature	Label/Tagged ID	Label/Extended Tagged ID	Icon	LED Behavior
Flash	Flash/ TAGS_FLASH_ 41 TAGS_Flash[]	—	Default	—
Login	Login/ TAGS_LOGIN_ 42 TAGS_Login[]	—	Default	—
TrnsfVM	TrnsfVM/SkTrnsfVMTag 0x3e	—	Default	—
LiveRcd	LiveRcd	—	Default	—
Night Service	Night Service/ TAGS_Night_Service[]	—	Radio Button	On—active Off—inactive
Myphoneapp URL service	My Phone Apps	—	URL service	—
EM URL service	Extension Mobility	—	URL service	—
SN URL service	Single Number Reach	—	URL service	—
Customized URL	The configured name	—	URL service	—

Configure Softkeys

Modify Softkey Display on SCCP Phone

To modify the display of softkeys, perform the following steps.

Restriction

- Enable the ConfList and MeetMe softkeys only if you have hardware conferencing configured. For information, see Meet-Me Conferencing in Cisco Unified CME 4.1 and Later versions, on page 1373 .
- The third softkey button on the Cisco Unified IP Phone 7905G and Cisco Unified IP Phone 7912G is reserved for the Message softkey. For these phones' templates, the third softkey button defaults to the Message softkey. For example, the **softkeys idle Redial Dnd Pickup Login Gpickup** command configuration displays, in order, the Redial, DND, Message, PickUp, Login, and GPickUp softkeys.
- The NewCall softkey cannot be disabled on the Cisco Unified IP Phone 7905G or Cisco Unified IP Phone 7912G.

Before You Begin

- Cisco CME 3.2 or a later version.
- Cisco Unified CME 4.2 or a later version to enable softkeys during the ringing call state.
- Cisco Unified CME 4.3 or a later version to enable softkeys during the remote-in-use state.
- The HLog softkey must be enabled with the **hunt-group logout HLog** command before it will be displayed. For more information, see Configure Ephone-Hunt Groups on SCCP Phones, on page 1291 .
- The Flash softkey must be enabled with the **fxo hook-flash** command before it will be displayed. For configuration information, see Enable Flash Softkey, on page 945 .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **softkeys alerting** {[**Acct**] [**Callback**] [**Endcall**]}
5. **softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**Hlog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [Trnsfer]}
6. **softkeys hold** {[**Join**] [**Newcall**] [**Resume**] [**Select**]}
7. **softkeys idle** {[**Cfwdall**] [**ConfList**] [**Dnd**] [**Gpickup**] [**Hlog**] [**Join**] [**Login**] [**Newcall**] [**Pickup**] [**Redial**] [**RmLstC**]}
8. **softkeys remote-in-use** {[**CBarge**] [**Newcall**]}
9. **softkeys ringing** {[**Answer**] [**Dnd**] [**HLog**]}
10. **softkeys seized** {[**CallBack**] [**Cfwdall**] [**Endcall**] [**Gpickup**] [**Hlog**] [**MeetMe**] [**Pickup**] [**Redial**]}
11. **exit**
12. **ephone** *phone-tag*
13. **ephone-template** *template-tag*
14. **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-template** *template-tag* **Example:** `Router(config)# ephone-template 15`	Enters ephone-template configuration mode to create an ephone template. • template-tag—Unique identifier for the ephone template that is being created. Range is 1 to 20.
Step 4	**softkeys alerting** {[**Acct**] [**Callback**] [**Endcall**]} **Example:** `Router(config-ephone-template)# softkeys alerting Callback Endcall`	(Optional) Configures an ephone template for softkey display during the alerting call state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 5	**softkeys connected** {[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**Hlog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [Trnsfer]} **Example:** `Router(config-ephone-template)# softkeys connected Endcall Hold Transfer Hlog`	(Optional) Configures an ephone template for softkey display during the call-connected state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 6	**softkeys hold** {[**Join**] [**Newcall**] [**Resume**] [**Select**]} **Example:** `Router(config-ephone-template)# softkeys hold Resume`	(Optional) Configures an ephone template for softkey display during the call-hold state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 7	**softkeys idle** {[**Cfwdall**] [**ConfList**] [**Dnd**] [**Gpickup**] [**Hlog**] [**Join**] [**Login**] [**Newcall**] [**Pickup**] [**Redial**] [**RmLstC**]} **Example:** `Router(config-ephone-template)# softkeys idle Newcall Redial Pickup Cfwdall Hlog`	(Optional) Configures an ephone template for softkey display during the idle state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.

	Command or Action	Purpose
Step 8	**softkeys remote-in-use** {[**CBarge**] [**Newcall**]} **Example:** `Router(config-ephone-template)# softkeys remote-in-use CBarge Newcall`	Modifies the order and type of softkeys that display on an IP phone during the remote-in-use call state.
Step 9	**softkeys ringing** {[**Answer**] [**Dnd**] [**HLog**]} **Example:** `Router(config-ephone-template)# softkeys ringing Answer Dnd Hlog`	(Optional) Configures an ephone template for softkey display during the ringing state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 10	**softkeys seized** {[**CallBack**] [**Cfwdall**] [**Endcall**] [**Gpickup**] [**Hlog**] [**MeetMe**] [**Pickup**] [**Redial**]} **Example:** `Router(config-ephone-template)# softkeys seized Endcall Redial Pickup Cfwdall Hlog`	(Optional) Configures an ephone template for softkey display during the seized state. • You can enter any of the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 11	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 12	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode. • phone-tag—Unique sequence number that identifies this ephone during configuration tasks.
Step 13	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 15`	Applies an ephone template to the ephone that is being configured.
Step 14	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done modifying the parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for SCCP Phones, on page 388.

Modify Softkey Display on SIP Phone

Restriction

- This feature is supported only for Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.
- You can download a custom softkey XML file from a TFTP server. However, if the softkey XML file contains an error, the softkeys might not work properly on the phone. We recommend the following procedure for creating a softkey template in Cisco Unified CME.
- HLog softkey is supported only on Cisco Unified IP Phones 7800 and 8800 series.

Before You Begin

Cisco Unified CME 4.1 or a later version. From Cisco Unified CME Release 11.6 onwards, HLog softkey is supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **softkeys connected** {[**Confrn**] [**Endcall**] [**Hold**] [**Trnsfer**] [**HLog**] }
5. **softkeys hold** {[**Newcall**] {**Resume**]}
6. **softkeys idle** {[**Cfwdall**] [**Newcall**] [**Redial**] [**HLog**] }
7. **softkeys seized** {[**Cfwdall**] [**Endcall**] [**Redial**]}
8. **exit**
9. **voice register pool** *pool-tag*
10. **template** *template-tag*
11. **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.

	Command or Action	Purpose
Step 3	**voice register template** *template-tag* **Example:** `Router(config)# voice register template 9`	Enters voice register template configuration mode to create a SIP phone template. • *template-tag*—Range: 1 to 10.
Step 4	**softkeys connected** {[**Confrn**] [**Endcall**] [**Hold**] [**Trnsfer**] [**HLog**] } **Example:** `Router(config-register-template)# softkeys connected Endcall Hold Transfer HLog`	(Optional) Configures a SIP phone template for softkey display during the call-connected state. • You can enter the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 5	**softkeys hold** {[**Newcall**] {**Resume**]} **Example:** `Router(config-register-template)# softkeys hold Resume`	(Optional) Configures a phone template for softkey display during the call-hold state. • Default is that the NewCall and Resume softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 6	**softkeys idle** {[**Cfwdall**] [**Newcall**] [**Redial**] [**HLog**] } **Example:** `Router(config-register-template)# softkeys idle Newcall Redial Cfwdall HLog`	(Optional) Configures a phone template for softkey display during the idle state. • You can enter the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 7	**softkeys seized** {[**Cfwdall**] [**Endcall**] [**Redial**]} **Example:** `Router(config-register-template)# softkeys seized Endcall Redial Cfwdall`	(Optional) Configures a phone template for softkey display during the seized state. • You can enter the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 8	**exit** **Example:** `Router(config-register-template)# exit`	Exits voice register template configuration mode.
Step 9	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 36`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 10	**template** *template-tag*	Applies a SIP phone template to the phone you are configuring.

	Command or Action	Purpose
	Example: `Router(config-register-pool)# template 9`	• *template-tag*— Template tag that was created with the **voice register template** command in Step 3 .
Step 11	**end** **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.

What to Do Next

If you are done modifying the parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391 .

Verify Softkey Configuration

Step 1 **show running-config**

Use this command to verify your configuration. In the following example, the softkey display is modified in phone template 7 and the template is applied to SIP phone 2. All other phones use the default arrangement of softkeys.

Example:

```
Router# show running-config
!
voice register dn 1 dual-line
 ring feature secondary
 number 126 secondary 1261
 description Sales
 name Smith
 call-forward busy 500 secondary
 call-forward noan 500 timeout 10
 huntstop channel
 no huntstop
 no forward local-calls
!
!
voice register template 7
 session-transport tcp
 softkeys hold Resume Newcall
 softkeys idle Newcall Redial Cfwdall HLog
 softkeys connected Endcall Trnsfer Confrn Hold Hlog
 voicemail 52001 timeout 30
.
.
.
voice register pool 2
 id mac 0030.94C2.A22A
 number 1 dn 4
 template 7
```

```
 dialplan 3
!
```

Step 2 **show telephony-service ephone-template** or **show voice register template** *template-tag*

Example:

These commands display the contents of individual templates.

```
Router# show telephony-service ephone-template
ephone-template 1
softkey ringing Answer Dnd
conference drop-mode never
conference add-mode all
conference admin: No
Always send media packets to this router: No
Preferred codec: g711ulaw
User Locale: US
Network Locale: US
```

or

```
Router# show voice register template 7
Temp Tag 7
Config:
 Attended Transfer is enabled
 Blind Transfer is enabled
 Semi-attended Transfer is enabled
 Conference is enabled
 Caller-ID block is disabled
 DnD control is enabled
 Anonymous call block is disabled
 Voicemail is 52001, timeout 30
 KPML is disabled
 Transport type is tcp
 softkey connected Endcall Trnsfer Confrn Hold HLog
 softkey hold Resume Newcall
 softkey idle Newcall Redial Cfwdall HLog
```

Enable Flash Softkey

Restriction The IP phone must support softkey display.

Before You Begin

To enable the Flash softkey, perform the following steps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **fxo hook-flash**
5. **restart all**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**fxo hook-flash** **Example:** `Router(config-telephony)#` **fxo hook-flash**	Enables the Flash softkey on phones that support softkey display on PSTN calls using an FXO port. **Note** The Flash softkey display is automatically disabled for local IP-phone-to-IP-phone calls.
Step 5	**restart all** **Example:** `Router(config-telephony)# restart all`	Performs a fast reboot of all phones associated with this Cisco Unified CME router. Does not contact the DHCP or TFTP server for updated information.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify Flash Softkey Configuration

Step 1 Use the **show running-config** command to display an entire configuration, including Flash softkey, which is listed in the telephony-service portion of the output.

Example:

```
Router# show running-config
telephony-service
 fxo hook-flash
 load 7960-7940 P00305000600
 load 7914 S00103020002
 max-ephones 100
 max-dn 500
```

Step 2 Use the **show telephony-service** command to show only the telephony-service portion of the configuration.

Configure Feature Blocking

To configure feature blocking for SCCP phones, perform the following steps.

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **features blocked** [**CFwdAll**] [**Confrn**] [**GpickUp**] [**Park**] [**PickUp**] [**Trnsfer**]
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
8. **restart**
9. Repeat Step 5 to Step 8 for each phone to which the template should be applied.
10. **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-template** *template-tag* **Example:** `Router(config)# ephone-template 1`	Enters ephone-template configuration mode. • *template-tag*—Unique sequence number that identifies this template during configuration tasks. Range is 1 to 20.
Step 4	**features blocked** [**CFwdAll**] [**Confrn**] [**GpickUp**] [**Park**] [**PickUp**] [**Trnsfer**] **Example:** `Router(config-ephone-template)# features blocked Park Trnsfer`	Prevents the specified softkey from invoking its feature. • **CFwdAll**—Call forward all calls. • **Confrn**—Conference. • **GpickUp**—Group call pickup.

	Command or Action	Purpose
		• **Park—**Call park. • **PickUp—**Directed or local call pickup. This includes pickup last-parked call and pickup from another extension or park slot. • **Trnsfer—**Call transfer.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 25`	Enters ephone configuration mode. • *phone-tag***—**Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones for a particular Cisco Unified CME system is version- and platform-specific. For the range of values, see the CLI help.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 1`	Applies an ephone template to an ephone. • *template-tag***—**Template number that you want to apply to this ephone. **Note** To view your ephone-template configurations, use the **show telephony-service ephone-template** command.
Step 8	**restart** **Example:** `Router(config-ephone)# restart`	Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information. **Note** If you are applying the template to more than one ephone, you can use the **restart all** command in telephony-service configuration mode to reboot all the phones so they have the new template information.
Step 9	Repeat Step 5 to Step 8 for each phone to which the template should be applied.	—
Step 10	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verify Block Softkey Configuration

Step 1 Use the **show running-config** command to display the running configuration, including ephone templates and ephone configurations.

Step 2 Use the **show telephony-service ephone-template** command and the **show telephony-service ephone** command to display only the contents of ephone templates and the ephone configurations, respectively.

Configure Immediate Divert (iDivert) Softkey on SIP Phone

To configure iDivert softkey (in connected state) on Cisco Unified SIP IP phones, perform the following step.

Note When one participant in a conference (Meetme, Ad Hoc, cBarge, or Join) presses the iDivert softkey, all remaining participants receive an outgoing greeting of the participant who pressed iDivert softkey.

Restriction

- iDivert feature is disabled when **call-forward all** is activated for a phone.
- iDivert feature is not activated for the second call when **call-forward busy** is activated for a phone and the phone is busy with the first call.
- If iDivert softkey is pressed before call forward no answer (CFNA) timeout, then the call is forwarded to voice mail.
- The calling and called parties can divert the call to their voice messaging mailboxes if both the parties press the iDivert softkey at the same time. The voice messaging mailbox of the calling party will receive a portion of the outgoing greeting of the called party. Similarly, the voice messaging mailbox of the called party will receive a portion of the outgoing greeting of the calling party.
- iDivert softkey is not supported when SIP phones fall back to SRST mode in Cisco Unified CME.
- iDivert after connect towards the voicemail with transcoding is not supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **softkeys connected [Confrn] [Endcall] [Hold] [Trnsfer] [iDivert]**
5. **softkeys hold [Newcall] {Resume] [iDivert]**
6. **softkeys ringing [Answer] [DND] [iDivert]**
7. **exit**
8. **voice register pool** *pool-tag*
9. **template** *template-tag*
10. **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 register template** *template-tag* **Example:** `Router(config)# voice register template 9`	Enters voice register template configuration mode to create a SIP phone template. • *template-tag*—Range: 1 to 10.
Step 4	**softkeys connected [Confrn] [Endcall] [Hold] [Trnsfer] [iDivert]** **Example:** `Router(config-register-template)# softkeys connected Endcall Hold Transfer iDivert`	(Optional) Configures a SIP phone template for softkey display during the call-connected state. • You can enter the keywords in any order. • Default is all softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.
Step 5	**softkeys hold [Newcall] {Resume] [iDivert]** **Example:** `Router(config-register-template)# softkeys hold Newcall Resume`	(Optional) Configures a phone template for softkey display during the call-hold state. • Default is that the NewCall and Resume softkeys are displayed in alphabetical order. • Any softkey that is not explicitly defined is disabled.

	Command or Action	Purpose
Step 6	**softkeys ringing [Answer] [DND] [iDivert]** **Example:** `Router(config-register-temp)# softkeys ringin dnd answer idivert`	Modifies the order and type of softkeys that display on a SIP phone during the ringing call state.
Step 7	**exit** **Example:** `Router(config-register-template)# exit`	Exits voice register template configuration mode.
Step 8	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 36`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 9	**template** *template-tag* **Example:** `Router(config-register-pool)# template 9`	Applies a SIP phone template to the phone you are configuring. • *template-tag*— Template tag that was created with the voice register template command in Step 3 .
Step 10	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode.

Configure Service URL Line Key Button on SCCP Phone

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone template** *template-tag*
4. **url-button** *index* **type** | url [name]
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** template-tag
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone template** *template-tag* **Example:** `Router(config)# ephone template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.

Step 4	**url-button** *index* **type** | url [name]
	
	Example:
	`Router#(config-ephone-template)#url-button 1 myphoneapp`
	`Router(config-ephone-template)#url-button 2 em`
	`Router(config-ephone-template)#url-button 3 snr`
	`Router (config-ephone-template)#url-button 4 http://www.cisco.com`
		Configures a service URL button on a line key.
		• *index*—Unique index number. Range: 1 to 8.
		• **type**—Type of service URL button. The following types of service URL buttons are available:
		◦ myphoneapp: My phone application configured under phone user interface.
		◦ em: Extension Mobility.
		◦ snr: Single Number Reach.
		• *url name*—Service URL with maximum length of 31 characters.

Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)#ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** template-tag **Example:** `Router(config-ephone)# ephone-template 5`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done configuring the URL buttons for phones in Cisco Unified CME, restart the phones.

Configure Service URL Line Key Button on SIP Phone

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **url-button** [**index** *number*] [**url** *location*] [**url** *name*]
5. **exit**
6. **voice register pool** *phone-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters voice register template configuration mode to create a SIP phone template. • *template-tag*—Unique identifier for the template that is being created. Range: 1 to 10.
Step 4	**url-button** [**index** *number*] [**url** *location*] [**url** *name*] **Example:** `Router(config-register-temp)url-button 1 http:// www.cisco.com`	Configures a service URL button on a line key. • **index** *number*—Unique index number. Range: 1 to 8. • **url** *location*—Location of the URL. • **url** *name*—Service URL with maximum length of 31 characters.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-register-temp)# exit`	Exits voice register template configuration mode.
Step 6	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 12`	Enters voice register pool configuration mode. • *phone-tag*—Unique number that identifies this voice register pool during configuration tasks.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the SIP phone template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done configuring the URL buttons for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Configure Feature Buttons on SCCP Phone Line Key

Restriction

- Answer, Select, cBarge, Join, and Resume features are not supported as PLKs.
- Feature buttons are only supported on Cisco Unified IP Phones 6911, 7941, 7942, 7945, 7961, 7962, 7965. 7970, 7971, and 7975 with SCCP v12 or later versions.
- Any features available through hard buttons are not provisioned. Use the `show ephone register detail` command to verify why the features buttons are not provisioned.
- Not all feature buttons are supported on Cisco Unified IP Phone 6911 phone. Call Forward, Pickup, Group Pickup, and MeetMe are the only feature buttons supported on the Cisco Unified IP Phone 6911.
- The **privacy-button** command is available on Cisco Unified IP phones running a SCCP Version 8 or later versions. The **privacy-buttton** command is overridden by any other available feature buttons.
- Locales are not supported on Cisco Unified IP Phone 7914.
- Locales are not supported for Cancel Call Waiting or Live Recording feature buttons.
- The feature state for DnD, Hlog, Privacy, Login, and Night Service feature buttons are indicated by an LED. For a list of LED behavior for PLK, see Table 81: LED Behavior, on page 936

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone template** *template-tag*
4. **feature-button index** *<feature identifier>* [**label** *<label>*]
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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.

	Command or Action	Purpose
Step 3	**ephone template** *template-tag* **Example:** `Router(config)# ephone template 10`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*- Unique identifier for the ephone template that is being created. Range: 1 to 10
Step 4	**feature-button index** <*feature identifier*> [**label** <*label*>] **Example:** `Router(config-ephone-template)feature-button 1 label hold`	Configures a feature button on a line key. • *index*- Index number, one from 25 for a specific feature type. • *feature identifier*-Feature ID or stimulus ID. • **label** -Non-default text label.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 5`	Enters ephone configuration mode. • *phone-tag*- Unique sequence number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 10`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done configuring the feature buttons for phones in Cisco Unified CME, restart the phones.

Configure Feature Buttons on SIP Phone Line Key

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **feature-button** [*index*] [*feature identifier*]
5. **exit**
6. **voice register pool** *phone-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters voice register template configuration mode to create a SIP phone template. • *template-tag* -Unique identifier for the template that is being created. Range: 1 to 10. **Note** Feature button can be configured under voice register pool or voice register template configuration mode. If both configurations are applied, the feature button configuration under voice register pool takes precedence.

Step 4	**feature-button** [*index*] [*feature identifier*]
	
	Example:
	`Router(config-voice-register-template)feature-button 1 DnD`
	`Router(config-voice-register-template)feature-button 2 EndCall`
	`Router(config-voice-register-template)feature-button 3 Cfwdall`
		Configures a feature button on a line key.
		• *index*—One of the 12 index numbers for a specific feature type.
		• *feature identifier* —Unique identifier for a feature. One of the following feature or stimulus IDs: Redial, Hold, Trnsfer, Cfwdall, Privacy, MeetMe, Confrn, Park, Pickup. Gpickup, Mobility, Dnd, ConfList,

	Command or Action	Purpose
		RmLstC, CallBack, NewCall, EndCall, HLog, NiteSrv, Acct, Flash, Login, TrnsfVM, or LiveRcd.
Step 5	**exit** **Example:** `Router(config-register-temp)# exit`	Exits voice register template configuration mode.
Step 6	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 12`	Enters voice register pool configuration mode. • *phone-tag*—Unique number that identifies this voice register pool during configuration tasks.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done configuring the feature buttons for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391

Configuration Example for Softkeys

Example for Modifying Softkey Display

The following example modifies the softkey display on four phones by creating two ephone templates. Ephone template 1 is applied to ephone 11, 13, and 15. Template 2 is applied to ephone 34. The softkey displays on all other phones use the default arrangement of keys.

```
ephone-template 1

 softkeys idle Redial Newcall
 softkeys connected Endcall Hold Trnsfer
ephone-template 2

 softkeys idle Redial Newcall
 softkeys seized Redial Endcall Pickup
```

```
 softkeys alerting Redial Endcall
 softkeys connected Endcall Hold Trnsfer
ephone 11
 ephone-template 1
ephone 13
 ephone-template 1
ephone 15
 ephone-template 1
ephone 34
 ephone-template 2
```

Example for Modifying HLog Softkey for SCCP Phones

The following example establishes the appearance and order of softkeys for phones that are configured with ephone-template 7. The Hlog key is available when a phone is idle, when it has seized a line, or when it is connected to a call. Phones without softkeys can use the standard HLog codes to toggle ready and not-ready status.

```
telephony-service
 hunt-group logout HLog
 fac standard
.
.
ephone-template 7
 softkeys connected Endcall Hold Transfer Hlog
 softkeys idle Newcall Redial Pickup Cfwdall Hlog
 softkeys seized Endcall Redial Pickup Cfwdall Hlog
```

Example for Modifying HLog Softkey for SIP Phones

The following example establishes the appearance and order of softkeys for phones that are configured with voice register template 7. The Hlog key is available when a phone is idle, when there is a ringIn, or when it is connected to a call. Phones without softkeys can use the standard HLog codes to toggle ready and not-ready status.

```
telephony-service
 hunt-group logout HLog
 fac standard
.
.
voice register template 7
 softkeys connected Endcall Hold Transfer Hlog
 softkeys idle Newcall Redial Pickup Cfwdall Hlog
 softkeys ringIn Answer DND iDivert Hlog
```

Example for Enabling Flash Softkey for PSTN Calls

The following example enables the Flash softkey for PSTN calls through an FXO voice port:

```
telephony-service
 fxo hook-flash
```

Example for Park and Transfer Blocking

The following example blocks the use of Park and Transfer softkeys on extension 2333:

```
ephone-template 1
 features blocked Park Trnsfer
ephone-dn 2
 number 2333
ephone 3
 button 1:2
 ephone-template 1
```

Example for Conference Blocking

The following example blocks the conference feature on extension 2579, which is on an analog phone:

```
ephone-template 1
 features blocked Confrn

ephone-dn 78
 number 2579

ephone 3
 ephone-template 1
 mac-address C910.8E47.1282
 type anl
 button 1:78
```

Example for Immediate Divert (iDivert) Configuration

The following example shows iDivert softkey in connected state:

```
Router# show voice register template 1
Temp Tag 1
Config:
  Attended Transfer is enabled
  Blind Transfer is enabled
  Semi-attended Transfer is enabled
Conference is enabled
  Caller-ID block is disabled
  DnD control is enabled
  Anonymous call block is disabled
  Softkeys connected iDivert
```

Example for Configuring URL Buttons on a SCCP Phone Line Key

The following example shows three URL buttons configured for line keys:

```
!
!
!
ephone-template  5
 url-button 1 em
 url-button 2 mphoneapp mphoneapp
 url-button 3 snr
!
ephone  36
 ephone-template 5
```

Example for Configuring URL Buttons on a SIP Phone Line Key

The following example shows URL buttons configured in voice register template 1:

```
Router# show run!voice register template  1
url-button 1 http://9.10.10.254:80/localdirectory/query My_Dir
url-button 5 http://www.yahoo.com Yahoo
!voice register pool  50
!
```

Example for Configuring Feature Button on a SCCP Phone Line Key

The following example shows feature buttons configured for line keys:

```
!
!
!
ephone-template  10
 feature-button 1 Park
 feature-button 2 MeetMe
 feature-button 3 CallBack
!
!
ephone-template 10
```

Example for Configuring Feature Button on a SIP Phone Line Key

The following example shows three feature buttons configured for line keys:

```
voice register template  5
 feature-button 1 DnD
 feature-button 2 EndCall
 feature-button 3 Cfwdall
 feature-button 4 HLog
!!
voice register pool 12
template 5
```

Note For more details on HLog functionality, see Call Coverage Features, on page 1239 chapter.

Where to Go Next

If you are done modifying the parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. For more information, see Generate Configuration Files for Phones, on page 388.

Ephone Templates

The **softkeys** commands are included in ephone templates that are applied to one or more individual ephones. For more information about templates, see Templates, on page 1427.

HLog Softkey

The HLog softkey must be enabled with the **hunt-group logout HLog** command before it will be displayed. For more information, see Configure Call Coverage Features, on page 1278.

Feature Information for Softkeys

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

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

Table 82: Feature Information for Softkeys

Feature Name	Cisco Unified CME Version	Feature Information
Account Code Entry	3.0	Account code entry was introduced.
Barge Softkey	4.3	The Barge, LiveRcd, and TrnsfVM softkeys were added.
Conferencing Softkeys	4.1	The ConfList, Join, MeetMe, RmLstC, and Select softkeys were added.
Feature Blocking	4.0	Feature blocking was introduced.
Feature Policy Softkey Control	8.5	Allows control display of softkeys on the Cisco Unified SIP IP Phones 8961, 9951, and 9971 using the feature policy template.
Flash Softkey	3.0	Flash softkey was introduced.
Immediate Divert Softkey for SIP Phones	8.5	Added support for iDivert softkey for SIP IP phones.
Programmable Line Keys	8.5	Allows you to configure a feature button or a URL button on a line key on both SIP and SCCP IP Phones.
Programmable Line Keys Enhancement	8.8	Adds support for softkeys as programmable line keys on Cisco Unified 6945, 8941, and 8945 SCCP IP Phones.
Programmable Line Keys for Cisco Unified SIP IP Phones	9.0	Adds support for softkeys as programmable line keys on Cisco Unified 6911, 6921, 6941, 6945, 6961, 8941, and 8945 SIP IP Phones.

Feature Name	Cisco Unified CME Version	Feature Information
Softkey Display	11.7	Support added for the softkeys 'Details' on Cisco IP Phone 7800 Series, and 'Show detail' on Cisco IP Phone 8800 Series.
	11.6	HLog Softkey support for SIP Phone was introduced.
	4.1	Configurable softkey display for IP phones running SIP is supported for the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE
	4.0	• An optional HLog softkey was added to the connected, idle, and seized call states. • The ability to customize softkey display in the hold call state was added.
	3.2	Configurable softkey display (the ability to customize softkey display in the alerting, connected, idle, and seized call states) was introduced.

CHAPTER 35

Speed Dial

Information About Speed Dial

Speed Dial Summary

Speed dial allows a phone user to quickly dial a number from a list. The different types of speed dial are summarized in Table 83: Speed Dial Types, on page 965.

Table 83: Speed Dial Types

Speed Dial Type	Availability of Numbers	Description	How Configured
Local Speed Dial Menu	System-level list of frequently called numbers that can be programmed on *all* phones. A maximum of 32 numbers can be defined. Numbers are set up by an administrator using an XML File speeddial.xml, which is placed in the Cisco Unified CME router's flash memory.	Users invoke entries from the Directories > Local Speed Dial menu on IP phones.	Enable a Local Speed Dial Menu, on page 970

Speed Dial Type	Availability of Numbers	Description	How Configured
Personal Speed Dial Menu	Speed dial entries are local to a specific IP phone. A maximum of 24 numbers per phone can be defined.	Users invoke entries from the Directories > Local Services > Personal Speed Dials menu on IP phones.	• Enable a Personal Speed Dial Menu on SCCP Phones, on page 972 • Enable a Personal Speed Dial Menu on SIP Phones, on page 980
Speed Dial Buttons and Abbreviated Dialing	Up to 99 speed-dial codes per phone.	For IP phones, the first entries that are set up occupy any unused line buttons and are invoked when a user presses one of these line buttons. Subsequent entries are invoked when a phone user dials the speed-dial code (tag) and the Abbr soft key. **Note** The feature to invoke subsequent entries by dialing the speed-dial code (tag) and the Abbr soft key is supported only on SCCP phones. Analog phone users invoke speed dial by entering an asterisk and the speed-dial code (tag) number of the desired entry.	• Define Speed-Dial Buttons and Abbreviated Dialing on SCCP Phones, on page 974 • Define Speed-Dial Buttons on SIP Phones, on page 979
Bulk-Loading Speed Dial Numbers	There can be up to ten text files containing lists of many speed-dial numbers that are loaded into flash, slot, or TFTP locations to be accessed by phone users. The ten files can hold 10,000 numbers.	Phone users dial the following sequence: *prefix-code list-id index* [*extension-digits*]	Enable Bulk-Loading Speed-Dial, on page 976

Speed Dial Type	Availability of Numbers	Description	How Configured
Monitor-Line Button for Speed Dial	Speed dial entries are local to a specific IP phone. There can be as many numbers as there are monitor lines on a phone.	IP phone buttons that are configured as monitor lines can be used to speed-dial the line that is being monitored.	No additional configuration required.
Direct Station Select (DSS) Service	All phones on which speed-dial line or monitor line button is configured.	Allows phone user to fast transfer a call by pressing a single speed-dial line or monitor line button.	Enable DSS Service, on page 971

Speed Dial Buttons and Abbreviated Dialing

In a Cisco Unified CME system, each phone can have up to 32 local speed-dial numbers (codes 1 to 32), up to 99 system-level speed-dial numbers (codes 1 to 99), or a combination of the two. If you program both a local and a system-level speed-dial number with the same speed-dial code (tag), the local number takes precedence. Typically you will want to reserve codes 1 to 32 for local, per-phone speed-dial numbers and use codes 33 to 99 for system-level speed-dial numbers so that there is no conflict.

On an IP phone, speed-dial entries are assigned to unused line buttons. Then, after all line buttons are used, subsequent entries are added but do not have an assigned line button. The speed-dial entry is not related to the physical button layout of the phone. Entries are assigned in order of speed-dial tag.

You can create local speed-dial codes with locked numbers that cannot be changed from the phone. You can also create empty local speed-dial codes on an IP phone without a telephone number. These empty speed-dial codes can be changed by the phone user to add a telephone number.

Changes to speed-dial entries are saved into the router's nonvolatile random-access memory (NVRAM) configuration after a timer-based delay.

For configuration information, see Define Speed-Dial Buttons and Abbreviated Dialing on SCCP Phones, on page 974.

Bulk-Loading Speed Dial Numbers

In Cisco Unified CME 4.0 and later versions, up to ten text files containing lists of many speed-dial numbers can be loaded into flash, slot, or TFTP locations to be accessed by phone users. The ten files can hold a total of up to 10,000 numbers. Each list holds numbers that are in an appropriate format for dialing from IP phones and SCCP-enabled analog phones.

Up to ten bulk speed-dial lists can be created. These lists might be corporate directory lists, regional lists, or local lists, for example. The speed-dial numbers in these lists can be system-level (available to all ephones) or personal (available to one or more specified ephones). Each list receives a unique speed-dial list ID number (sd-id) between 0 and 9.

Speed-dial list ID numbers that are not used for global speed-dial lists are available to identify personal, custom lists that are associated with individual phones.

Bulk speed-dial lists contain entries of speed-dial codes and the associated phone numbers to dial. Each entry in a speed-dial list must appear on a separate line. The fields in each entry are separated by commas (,). A line that begins with a semicolon (;) is handled as a comment. The format of each entry is shown in the following line.

index,*digits*,[*name*],[**hide**],[**append**]

Table 84: Bulk Speed-Dial List Entry, on page 968 explains the fields in a bulk speed-dial list entry.

Table 84: Bulk Speed-Dial List Entry

Field	Description
index	Zero-filled number that uniquely identifies this index entry. Maximum length: 4 digits. All index entries must be the same length.
digits	Telephone number to dialed. Represents a fully qualified E.164 number. Use a comma (,) to represent a one-second pause.
name	(Optional) Alphanumeric string to identify a name, up to 30 characters.
hide	(Optional) Enter **hide** to block the display of the dialed number.
append	(Optional) Enter **append** to allow additional digits to be appended to this number when dialed.

The following is a sample bulk speed-dial list:

```
01,5550140,voicemail,hide,append
90,914085550153,Cisco extension,hide,append
11,9911,emergency,hide,
91,9911,emergency,hide,
08,110,Paging,,append
```

To place a call to a speed-dial entry in a list, the phone user must first dial a prefix, followed by the list ID number, then the index for the bulk speed-dial list entry to be called.

For configuration information, see Enable Bulk-Loading Speed-Dial, on page 976.

Monitor-Line Button for Speed Dial

For Cisco CME 3.2 and later versions, a monitor-line button can be used to speed-dial the monitor line’s number. A monitor line is a line that is shared by two people. Only one person can make and receive calls on the shared line at a time, while the other person, whose line is in monitor mode, is able to see that the line is in use. Speed dialing is available when monitor lines’ lamps are off, indicating that the line is not in use. For example, an assistant who wants to talk with a manager can press an unlit monitor-line button to speed-dial the manager’s number.

A monitor-line lamp is off or unlit only when its line is in the idle call state. The idle state occurs before a call is made and after a call is completed. For all other call states, the monitor-line lamp is on or lit.

The following example shows a monitor-line configuration. Extension 2311 is the manager's line, and ephone 1 is the manager's phone. The manager's assistant monitors extension 2311 on button 2 of ephone 2. When the manager is on the line, the lamp is lit on the assistant's phone. If the lamp is not lit, the assistant can speed-dial the manager by pressing button 2.

```
ephone-dn 11
   number 2311

  ephone-dn 22
   number 2322

  ephone 1
   button 1:11

  ephone 2
   button 1:22 2m11
```

No additional configuration is required to enable a phone user to speed dial the number of a monitored shared line, when the monitored line is in an idle call state.

DSS (Direct Station Select) Service

In Cisco Unified CME 4.0(2) and later versions, the DSS (Direct Station Select) Service feature allows the phone user to press a single speed-dial line button to transfer an incoming call when the call is in the connected state. This feature is supported on all phones on which monitor line buttons for speed dial or speed-dial line buttons are configured.

When the DSS service is enabled, the system automatically generates a simulated transfer key event when needed, eliminating the requirement for the phone user to press the Transfer button.

Disabling the service changes the behavior of the speed-dial line button on all IP phones so that a user pressing a speed-dial button in the middle of a connected call will play out the speed-dial digits into the call without transferring the call. When DSS service is disabled, the phone user must first press Transfer and then press the monitor or speed-dial line button to transfer the incoming call.

For configuration information, see Enable a Local Speed Dial Menu, on page 970.

Phone User-Interface for Speed Dial and Fast Dial

In Cisco Unified CME 4.3 and later versions, IP phone users can configure their own speed-dial and fast-dial settings directly from the phone. The speed-dial and fast-dial settings can be added or modified on the phone by using a menu available with the Services feature button. Extension Mobility users can add or modify speed-dial settings in their user profile after logging in. Fast-dial settings are not configurable from Extension Mobility phones, nor is the logout profile configurable from the phone.

Previously, the speed-dial and fast-dial configuration for a phone could only be done in Cisco Unified CME or by using the web-based GUI. This feature gives phone users the convenience of configuring their speed-dial and fast-dial settings from their phones directly.

The speed-dial and fast-dial user interface is enabled by default on all phones with displays. You can disable the capability for an individual phone in Cisco Unified CME to prevent a phone user from accessing the interface. If a phone's speed-dial or fast-dial setting is configured with an ephone-template, the configuration from the phone applies only to the specific phone and does not change the ephone-template configuration.

For configuration information, see Enable Phone User Interface for Configuring Speed-Dial and Fast-Dial, on page 978.

For information on how phone users configure speed-dial and fast-dial buttons using the phone user-interface, see the Cisco Unified IP Phone documentation for Cisco Unified CME.

Configure Speed Dial

Enable a Local Speed Dial Menu

To enable a local speed-dial menu for all phones, SCCP and SIP, in Cisco Unified CME, perform the following steps:

Restriction

- If a speed dial XML file contains incomplete information, for example the name or telephone number is missing for an entry, any information in the file that is listed after the incomplete entry is not displayed when the local speed dial directory option is used on a phone.
- Before Cisco Unified CME 4.1, local speed-dial menu is not supported on SIP phones.
- Before Cisco CME 3.3, analog phones are limited to nine speed-dial numbers.

Before You Begin

An XML file called speeddial.xml must be created and copied to the TFTP server application on the Cisco Unified CME router. The contents of speeddial.xml must be valid as defined in the Cisco-specified directory DTD. See Example for Enabling a Local Speed Dial Menu, on page 982 and the Cisco Unified IP Phone Services Application Development Notes.

SUMMARY STEPS

1. **enable**
2. **copy tftp flash**
3. **configure terminal**
4. **ip http server**
5. **ip http path flash:**
6. **exit**

DETAILED STEPS

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

	Command or Action	Purpose

Step 2	**copy tftp flash**
	
	Example:
	`Router# copy tftp flash`
	`Address or name of remote host []? 172.24.59.11`
	`Source filename []? speeddial.xml`
	`Destination filename [speeddial.xml]?`
	`Accessing tftp://172.24.59.11/speeddial.xml...`
	`Erase flash:before copying? [confirm]n`
	`Loading speeddial.xml from 172.24.59.11 (via FastEthernet0/0):!`
	`[OK - 329 bytes]`
	`Verifying checksum...  OK (0xF5DB)`
	`329 bytes copied in 0.044 secs (7477 bytes/sec)`
		Copies the file from the TFTP server to the router flash memory.
		• At the first prompt, enter the IP address or the DNS name of the remote host.
		• At both filename prompts, enter speeddial.xml.
		• At the prompt to erase flash, enter no.

Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**ip http server** **Example:** `Router(config)# ip http server`	Enables the Cisco web-browser user interface on the router.
Step 5	**ip http path flash:** **Example:** `Router(config)# ip http path flash:`	Sets the base HTTP path to flash memory.
Step 6	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Enable DSS Service

To enable DSS Service for all on all SCCP phones on which monitor line buttons for speed dial or speed-dial line buttons are configured, perform the following steps.

Before You Begin

Cisco Unified CME 4.0(2) or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **service dss**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**service dss** **Example:** `Router(config-telephony)# service dss`	Configures DSS (Direct Station Select) service globally for all phone users in Cisco Unified CME.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Exits configuration mode and enters privileged EXEC mode.

Enable a Personal Speed Dial Menu on SCCP Phones

To enable a personal speed-dial menu, perform the following steps.

Restriction

- A personal speed-dial menu is available only on certain Cisco Unified IP phones, such as the 7940, 7960, 7960G, 7970G, and 7971G-GE. To determine whether personal speed-dial menu is supported on your IP phone, see the Cisco Unified CME User Guides for your IP phone model.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **fastdial** *dial-tag number* **name** *name-string*
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** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode. • *phone-tag*—Unique number of the phone for which you want to program personal speed-dial numbers.
Step 4	**fastdial** *dial-tag number* **name** *name-string* **Example:** `Router(config-ephone)#` **fastdial 1 5552 name Sales**	Creates an entry for a personal speed-dial number on this phone. • *dial-tag*—Unique identifier to identify this entry during configuration. Range is 1 to 100. **Note** The range for dial-tag is 1 to 24 for Cisco Unified CME versions earlier than 10.5 • *number*—Telephone number or extension to be dialed. • **name** *name-string*—Label to appear in the Personal Speed Dial menu, containing a string of up to 24 alphanumeric characters. Personal speed dial is handled through an XML request, so characters that have special meaning to HTTP, such as ampersand (&), percent sign (%), semicolon (;), angle brackets (< >), and vertical bars (||), are not allowed.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Define Speed-Dial Buttons and Abbreviated Dialing on SCCP Phones

To define speed-dial buttons and abbreviated dialing codes, perform the following steps for each speed-dial definition to be configured.

Restriction

- On-hook abbreviated dialing using the Abbr soft key is supported only on the following phones:
    - Cisco Unified IP Phone 7905G
    - Cisco Unified IP Phone 7912G
    - Cisco Unified IP Phone 7920G
    - Cisco Unified IP Phone 7970G
    - Cisco Unified IP Phone 7971G-GE
- System-level speed-dial codes cannot be changed by the phone user, at the phone.
- Before Cisco CME 3.3, analog phones were limited to nine speed-dial numbers.
- Before to Cisco CME 3.3, speed-dial entries that were in excess of the number of physical phone buttons available were ignored by IP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **speed-dial** *speed-tag digit-string* [**label** *label-text*]
5. **restart**
6. **exit**
7. **telephony-service**
8. **directory entry**{{*directory-tag number* **name** *name*}| **clear**}
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 55`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies the phone on which you are adding speed-dial capability.
Step 4	**speed-dial** *speed-tag digit-string* [**label** *label-text*] **Example:** `Router(config-ephone)# speed-dial 1 +5001 label "Head Office"`	Defines a unique speed-dial identifier, a digit string to dial, and an optional label to display next to the button. • *speed-tag*—identifier for a speed-dial definition. Range is 1 to 33.
Step 5	**restart** **Example:** `Router(config-ephone)# restart`	Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information.
Step 6	**exit** **Example:** `Router(config-ephone)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 7	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 8	**directory entry**{{*directory-tag number* **name** *name*}| **clear**} **Example:** `Router(config-telephony)# directory entry 45 8185550143 name Corp Acctg`	Adds a system-level directory and speed-dial definition. • *directory-tag*—Digit string that provides a unique identifier for this entry. Range is 1 to 99. If the same tags 1 through 33 are configured at a phone-level by using **speed-dial** command, and at a system-level by using this command, the local definition takes precedence. To prevent this conflict, we recommend that you use only codes 34 to 99 for system-level speed-dial numbers.
Step 9	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Enable Bulk-Loading Speed-Dial

To enable bulk-loading speed-dial numbers, perform the following steps:

Restriction

- Bulk speed dial is not supported on FXO trunk lines.

Before You Begin

- Cisco Unified CME 4.0 or a letter version.
- The bulk speed-dial text files containing the lists must be available in a location that is available to the Cisco Unified CME router: flash, slot, or TFTP location.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **bulk-speed-dial list** *list-id location*
5. **bulk-speed-dial prefix** *prefix-code*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**bulk-speed-dial list** *list-id location* **Example:** `Router(config-telephony)# bulk-speed-dial list 6 flash:sd_dept_0_1_8.txt`	identifies the location of a bulk speed-dial list. • *list-id*—Digit that identifies the list to be used. Range is 0 to 9.

	Command or Action	Purpose
		• *location*—Location of the bulk speed-dial text file in URL format. Valid storage locations are TFTP, Slot 0/1, and flash memory. This command can also be configured in ephone configuration mode for specific phones.
Step 5	**bulk-speed-dial prefix** *prefix-code* **Example:** `Router(config-telephony)# bulk-speed-dial prefix #7`	Sets the prefix code that phone users dial to access speed-dial numbers from a bulk speed-dial list. • *prefix-code*—One- or two-character access code for speed dial. Valid characters are digits from 0 to 9, asterisk (*), and pound sign (#). Default is #.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify Bulk Speed-Dial Parameters on SCCP Phones

show telephony-service bulk-speed-dial

Use this command to display information on speed-dial lists.

Example:

```
Router# show telephony-service bulk-speed-dial summary

  List-id    Entries      Size    Reference  url
        0         40      3840    Global     tftp://192.168.254.254/phonedirs/uut.csv
        1         20      1920    Global     phoneBook.csv
        8         15      1440    Global     tftp://192.168.254.254/phonedirs/big.txt
        9         20      1920    Global     tftp://192.168.254.254/phonedirs/phoneBook.csv
        6      24879   2388384    ephone-2   tftp://192.168.254.254/phonedirs/big.txt1
        7         20      1920    ephone-2   phoneBook.csv
        6      24879   2388384    ephone-3   big.txt1
        7         20      1920    ephone-3   phoneBook.csv

  4 Global List(s) 4 Local List(s)
```

Enable Phone User Interface for Configuring Speed-Dial and Fast-Dial

To enable a phone user to configure speed-dial and fast-dial numbers from a menu on their phone, perform the following steps. This feature is enabled by default. You must perform this task only if the feature was previously disabled on a phone.

Restriction Extension Mobility users cannot configure fast-dial settings (for personal speed-dial) from their phone.

Before You Begin

- Cisco Unified CME 4.3 or a later release.
- The Service URL must be configured. See Provision URLs for Feature Buttons for SCCP Phones, on page 1476.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **phone-ui speeddial-fastdial**
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** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 4	**phone-ui speeddial-fastdial** **Example:** `Router(config-ephone)# phone-ui speeddial-fastdial`	Enables a phone user to configure speed-dial and fast-dial numbers on their phone. • This command is enabled by default.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

What to Do Next

For information on how phone users configure speed dial and fast dial buttons using the UI, see Cisco Unified IP Phone documentation for Cisco Unified CME.

Define Speed-Dial Buttons on SIP Phones

To define speed-dial buttons for Cisco SIP Phones, perform the following steps.

Restriction

- Certain SIP phones, such as the Cisco Unified IP Phone 7960 and 7940, cannot be configured to enable speed dialing. Phone users with these phones must manually configure speed-dial numbers by using the user interface at their Cisco Unified IP phone.
- On Cisco Unified IP phones, speed-dial definitions are assigned to available buttons that have not been assigned to actual extensions. Speed-dial definitions are assigned in the order of their identifier numbers.
- Phones with Cisco ATA devices are limited to a maximum of nine speed-dial numbers. Speed-dial numbers cannot be programmed by using the user interface at the phone.

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **speed-dial** *speed-tag digit-string* [**label** *label-text*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router# enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 23`	Enters voice register pool configuration mode to set parameters for specified SIP phone.
Step 4	**speed-dial** *speed-tag digit-string* [**label** *label-text*] **Example:** `router(config-register-pool)# speed-dial 2 +5001 label "Head Office"`	Creates a speed-dial definition in Cisco Unified CME for a SIP phone or analog phone that uses an analog adapter (ATA). • *speed-tag*—Unique sequence number that identifies the speed-dial definition during configuration. Range is 1 to 5.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Examples

The following example shows how to set speed-dial button 2 to dial the head office at extension 5001 and locks the setting so that the phone user cannot change the setting at the phone:

```
Router(config)# voice register pool 23
Router(config-register-pool)# speed-dial 2 +5001 label "Head Office"
```

Enable a Personal Speed Dial Menu on SIP Phones

To enable a personal speed-dial menu, perform the following steps.

Restriction

- A personal speed-dial menu is available only on certain Cisco Unified IP phones, such as the 7811, 7821, 7841, 7861, 8841, and 8861. To determine whether personal speed-dial menu is supported on your IP phone, see the Cisco Unified CME User Guides for your IP phone model.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **fastdial** *entry-tag number* **name** *name-string*
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 register pool** *pool-tag* **Example:** `Router(config)# voice register pool 1`	Enters voice-register pool configuration mode. • **pool-tag—**Unique number of the phone for which you want to program personal speed-dial numbers.
Step 4	**fastdial** *entry-tag number* **name** *name-string* **Example:** `Router(config-register-pool)#` **fastdial 1 5552 name Sales**	Creates an entry for a personal speed-dial number on this phone. • *entry-tag*—Unique identifier to identify this entry during configuration. Range is 1 to 100. **Note** The range for entry-tag is 1 to 24 for Cisco Unified CME versions earlier than 10.5. • *number*—Telephone number or extension to be dialed. • **name** *name-string*—Label to appear in the Personal Speed Dial menu, containing a string of up to 24 alphanumeric characters. Personal speed dial is handled through an XML request, so characters that have special meaning to HTTP, such as ampersand (&), percent sign (%), semicolon (;), angle brackets (< >), and vertical bars (||), are not allowed.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Configuration Examples for Speed Dial

Example for Enabling a Local Speed Dial Menu

The following commands enable the Cisco web browser and set the HTTP path to flash memory so that the speeddial.xml file in flash memory is accessible to IP phones:

```
ip http server
ip http path flash:
```

The following XML file—speeddial.xml, defines three speed-dial numbers that will appear to the user after they press the Directories button on an IP phone.

```
<CiscoIPPhoneDirectory>
<Title>Local Speed Dial</Title>
<Prompt>Record 1 to 1 of 1 </Prompt>

<DirectoryEntry>
  <Name>Security</Name>
  <Telephone>71111</Telephone>
</DirectoryEntry>

<DirectoryEntry>
 <Name>Marketing</Name>
 <Telephone>71234</Telephone>
</DirectoryEntry>

<DirectoryEntry>
 <Name>Tech Support</Name>
  <Telephone>71432</Telephone>
</DirectoryEntry>

</CiscoIPPhoneDirectory>
```

Example for Configuring Personal Speed Dial Menu on SIP Phone

The following example creates a directory of three personal speed-dial listings for one IP phone:

```
ephone 1
   fastdial 1 5489 name Marketing
   fastdial 2 12125550155 name NY Sales
   fastdial 3 12135550112 name LA Sales
```

Example for Configuring Speed-Dial Buttons and Abbreviated Dialing

The following example defines two locked speed-dial numbers with labels to appear next to the speed-dial buttons on ephone 1. These speed-dial definitions are assigned to the next empty buttons after all extensions are assigned. For instance, if two extensions are assigned on the Cisco Unified IP Phones 7960 and 7960G, these speed-dial definitions appear on the third and fourth buttons.

This example also defines two system-level speed-dial numbers with the **directory entry** command. One is a local extension and the other is a ten-digit telephone number.

```
ephone 1
   mac-address 1234.5678.ABCD
   button 1:24 2:25
   speed-dial 1 +5002 label Receptionist
   speed-dial 2 +5001 label Security

  telephony-service
   directory entry 34 5003 name Accounting
   directory entry 45 8185550143 name Corp Acctg
```

Example for Configuring Bulk-Loading Speed Dial

The following example changes the default bulk speed-dial prefix to #7 and enables global bulk speed-dial list number 6 for all phones. It also enables a personal bulk speed-dial list for ephone 25.

```
telephony-service
   bulk-speed-dial list 6 flash:sd_dept_01_1_87.txt
   bulk-speed-dial prefix #7

  ephone-dn 3
   number 2555

  ephone-dn 4
   number 2557

  ephone 25
   button 1:3 2:4
   bulk-speed-dial list 7 flash:lmi_sd_list_08_24_95.txt
```

Example for Configuring Speed-Dial and Fast-Dial User Interface

The following example shows that the user interface for speed-dial and fast-dial configuration is disabled on phone 12:

```
ephone  12
   no phone-ui speeddial-fastdial
   ephone-template 5
   mac-address 000F.9054.31BD
   type 7960
   button  1:10 2:7
```

Where to Go Next

If you are finished creating or modifying speed-dial configurations for individual phones, you must reboot phones to download the modified configuration. See Reset and Restart Cisco Unified IP Phones, on page 397.

DSS Call Transfer

Monitor-line button speed dial, also known as direct station select (DSS) call transfer, allows you to use a monitored line button to speed-dial a call to that extension. If you want to allow consultation during DSS transfers, see Information About Call Transfer and Forward, on page 1147.

Feature Information for Speed Dial

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

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

Table 85: Feature Information for Speed Dial

Feature Name	Cisco Unified CME Version	Feature Information
Speed Dial	4.3	Added user interface on SCCP phones for programming Speed Dial and Fast Dial.
	4.1	Added support for local and personal speed-dial menus for SIP phones in Cisco Unified CME.
	4.0(2)	Added support for DSS Service which allows phone user to fast transfer a call by pressing a single speed-dial line or monitor line button.
	4.0	Added support for bulk speed-dial list for SCCP phones in Cisco Unified CME.
	3.4	Added support for speed dial buttons on SIP phones in Cisco Unified CME.
	3.0	• Added support for personal speed-dial from SCCP phones in Cisco Unified CME. • Number of speed-dial definitions that can be created was increased from 4 to 33. • The ability to program speed-dial numbers at the phone was introduced. • The ability to lock speed-dial numbers was introduced.
	1.0	Speed dial using the **speed-dial** command was introduced.

CHAPTER 36

Video Support

Prerequisites for Video Support

- H.323 or SIP network for voice calls is operational.
- Cisco Unified CME 4.0 or a later version.
- Cisco Unified IP phones are registered in Cisco Unified CME.
- Connection between Cisco Unified Video Advantage (CUVA) 1.02 or a later version and the Cisco Unified IP phone is up. From a PC with CUVA 1.02 or a later version installed, ensure that the line between the CUVA and the Cisco Unified IP phone is green. For more information, see Cisco Unified Video Advantage User Guide.
- Correct video firmware is installed on the Cisco Unified IP phone.
    - For Cisco Unified IP Phone 7940G and 7960G, 6.0(4) or a later version.
    - Cisco Unified IP Phone 7970G, 7.0(3) or a later version.
    - Cisco Unified IP Phone 7941G and7961G, 7.0(3) or a later version.

Note Other video-enabled endpoints registered with a Cisco Unified Communications Manager (Cisco Unified CM) can place video calls to Cisco Unified IP phones only if the phones are registered with a Cisco Unified CME and the appropriate video firmware is installed on the Cisco Unified IP phone.

Restrictions for Video Support

- This feature supports only the following video codecs:
  - H.261—Cisco Unified CME 4.0 and later versions
  - H.263—Cisco Unified CME 4.0 and later versions
  - H.264—Cisco Unified CME 7.1 and later versions
- This feature supports only the following video formats:
  - 4CIF—Resolution 704x576
  - 16CIF—Resolution 1408x1152
  - Common Intermediate Format (CIF)—Resolution 352x288
  - One-Quarter Common Intermediate Format (QCIF)—Resolution 176x144
  - Sub QIF (SQCIF)—Resolution 128x96
- The call start fast feature is not supported with an H.323 video connection. You must configure call start slow for H.323 video. For configuration information, see Enable Support for Video Streams Across H.323 Networks, on page 1000.
- Video capabilities are configured per phone, 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.
  - SIP endpoints— When a video-capable SCCP endpoint connects to a SIP endpoint, the call falls back to audio-only (prior to Cisco Unified CME 8.6).
  - Video supplementary services between Cisco Unified CME and Cisco Unified CM.
- If the Cisco Unified CM is configured for Media Termination Point (MTP) transcoding, a video call between Cisco Unified CME and Cisco Unified CM is not supported.
- Video telephony is not supported with Cisco Unified CME MTP and codec g729/dspfarm-assist configuration under ephone.
- If an SCCP endpoint calls an SCCP endpoint on the local Cisco Unified CME and one of the endpoints transferred across an H.323 network, a video-consult transfer between the Cisco Unified CME systems is not supported.

- 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.
- For Cisco Unified CME, the video capabilities in the vendor configuration firmware is a global configuration. This means that, although video can be enabled per ephone, the video icon shows on all Cisco Unified IP phones supported by Cisco Unified CME.
- Because of the extra CPU consumption on RTP-stream mixing, the number of video calls supported on Cisco Unified CME crossing an H.323 network is less than the maximum number of ephones supported.
- Cisco Unified CME cannot differentiate audio-only streams and audio-in-video streams. You must configure the DSCP values of audio and video streams in the H.323 dial-peers.
- If RSVP is enabled on the Cisco Unified CME, a video call is not supported.
- A separate VoIP dial peer, configured for fast-connect procedures, is required to complete a video call from a remote H.323 network to a Cisco Unity Express system.
- Video call is enabled on Cisco Unified CME, when the active call is held and resumed.

Information About Video Support

Video Support Overview

Video support allows you to pass a video stream, with a voice call, between two video-capable SCCP endpoints and between SCCP and H.323 endpoints. Through the Cisco Unified CME router, the video-capable endpoints can communicate with each other locally to a remote H.323 endpoint through a gateway or through an H.323 network.

Video capabilities are disabled by default, and enabling video capabilities on Cisco Unified CME does not automatically enable video on all ephones. You must first enable video globally for all video-capable SCCP phones associated with a Cisco Unified CME router and then enable video for each phone individually. Video parameters, like maximum bit rate, are set at a system level.

For information about the global configuration for video capabilities, see Enable System-Level Video Capabilities, on page 1002.

For information about configuring an individual phone for video capabilities, see Enable Video Capabilities on a Phone, on page 1003.

Note After video is enabled globally, all video-capable ephones display the video icon.

SIP Trunk Video Support

Cisco Unified CME 7.1 adds the following support for video calls:

- Support for video calls between SCCP endpoints across different Cisco Unified CME routers connected through a SIP trunk. All previously supported SCCP video endpoints and video codecs are supported.

- H.264 video support—H.264 provides high-quality images at low bit rates and is widely used in commercial video conferencing systems. The H.264 codec supports the following video calls:
    - SCCP to SCCP
    - SCCP to SIP
    - SCCP to H.323
    - Dynamic payload negotiation for H.264 (both SCCP to SIP and SCCP to H323)

Restriction

- On Cisco Unified CME 8.6, calls made from SIP endpoints across a SIP trunk terminating on a non-CME endpoint (such as those controlled by a Cisco Unified CM or video conferencing MTU) require the following CLI to be configured to allow video:

```
voice service voip
 sip
   asymmetric payload full
```

- The **no supplementary-service sip moved-temporarily** and **no supplementary-service sip refer** commands are not supported for video calls through a SIP trunk.
- Supplementary services like call hold, call resume and call transfer are not supported on video calls between SCCP and SIP endpoints that are registered with CME. The call gets converted into audio-only mode when these supplementary services are invoked.

No new configuration is required to support these enhancements. For configuration information, see Configure Video Support, on page 994.

Matching Endpoint Capabilities

During phone registration, information about endpoint capabilities is stored in the Cisco Unified CME. 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 become effective 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 each 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 CME 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 the call setup for video, media setup handling determines if a video-media-path is required. 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 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.

Because the endpoint capability negotiation and match occur after the H.323 connect message, video streams over H.323 network require slow-start on call setup procedures for Cisco Unified CME. An H.323 network can connect to a remote Cisco Unified CME router, Cisco Unified CM, remote IP to IP gateway, or a video-capable H.323 endpoint. For configuration information, see Enable System-Level Video Capabilities, on page 1002.

SIP Endpoint Video and Camera Support for Cisco Unified IP Phones 8961, 9951, and 9971

Cisco Unified CME 8.6 and later versions add phone-based video support and Universal Serial Bus (USB) camera support for Cisco Unified IP Phones 8961, 9951, and 9971. The Cisco Unified IP Phones 8961, 9951, and 9971 display local video using the USB camera. Cisco Unified IP Phones 9951 and 9971 with phone load 9.1.1 decode remote incoming video RTP streams and display the video on the phone's display screen. However, the video and USB camera capabilities of these two phones are disabled on Cisco Unified CME by default and are enabled by setting up the video and camera parameters in the phone provisioning file.

Cisco Unified CME 8.6 supports local SIP-video-to-SIP-video calls and SIP-video-to-SCCP-CUVA-video calls on Cisco Unified IP Phones 8961, 9951, and 9971 on the line side. On the trunk side, SIP video call is only supported with SIP trunk. H323 trunk is not supported for video calls on Cisco Unified IP Phones 9951 and 9971.

The media path for SIP video call is flow through and media flow-around is not supported for SIP line in Cisco Unified CME.

Video and Camera Configuration for Cisco Unified IP Phones

Cisco Unified CME uses the **video** and **camera** commands to allow video or camera to be enabled per phone, per template, or for global configuration. The **video** and **camera** commands are configured under the voice register pool, voice register template, and voice register global configuration modes. Once the commands are configured, the **create profile** command is required to have the phones provision file update with new configuration. For more information on enabling camera and video parameters on phones, see Enable Video and Camera Support on Cisco Unified SIP Phones, on page 994.

The changes in video and camera configuration are applied to the phones when Cisco Unified CME sends the request to a phone through a service-control event in a SIP NOTIFY message. In earlier versions of Cisco Unified CME, SIP phones were required to reset and restart to update the new configuration parameters.

In Cisco Unified CME 8.6 and later versions, you use the **apply-config** command under voice register pool and voice register global configuration modes to dynamically apply the video and camera configuration changes to the phone configuration of Cisco Unified IP Phones 8961, 9951, and 9971 without restarting or resetting the phones and without causing any service interruption.

When Cisco Unified IP Phones 8961, 9971 and 9951 receive the apply-config request, the phones retrieve the new configuration file from the TFTP server and compare it with the existing configuration. The phones may restart themselves if there are any changes that requires a restart; otherwise, the phones apply the changes dynamically without restarting.

For more information, see Apply Video and Camera Configuration to Cisco Unified SIP Phones, on page 997.

Bandwidth Control for SIP Video Calls

Video call bandwidth control is critical when there is a limit in resources. Typically, video calls require much higher bandwidth usage than audio-only calls. Video calls on Cisco Unified IP Phones 9951 and 9971 can use up to 1 Mbps for VGA quality video compared to 64 kbps plus overhead for a G711 audio call.

In Cisco Unified CME 8.6, the Cisco Unified SIP IP Phones 9951 and 9971 with VGA resolution offer 1-Mbps maximum bit-rate and answer with a lower value of received offer and 1 Mbps. Phones transmit video resolution and frame rate is set according to the maximum bandwidth bit-rate negotiated in the SIP offer or answer. Cisco Unified CME controls the SIP global bandwidth by configuring the **bandwidth video tias-modifier** *bandwidth value* [**negotiate** *end-to-end*] command in voice register global configuration mode. The bandwidth control configuration is applied to the SIP phone dial-peer.

There are no new bandwidth changes in the SCCP CUVA side and the bandwidth configuration works the same as in earlier versions of Cisco Unified CME.

For more information on configuring bandwidth control, see Configure Video Bandwidth Control for SIP to SIP Video Calls, on page 999.

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.
- With flow-through mode, the video media path is the same as for an audio call. Media packets flow through the gateway, thus hiding the networks from each other.

Use the **show voip rtp connection** command to display information about RTP named-event packets, such as caller-ID number, IP address, and port for both the local and remote endpoints, as shown in the following sample output:

```
Router# show voip rtp connections

  VoIP RTP active connections :
  No. Callid  dstCallid  LocalRTP RmtRTP LocalIP RemoteIP
  1   102     103        18714    18158  10.1.1.1 192.168.1.1
  2   105     104        17252    19088  10.1.1.1 192.168.1.1
  Found 2 active RTP connections
  ============================
```

Configure Video Support

Enable Video and Camera Support on Cisco Unified SIP Phones

To enable video and camera support on Cisco Unified SIP Phones such as 8845, 8865, 9951, and 9971, perform the following steps:

Note
- Shared line is not supported.
- Video transfer and forward supplementary service is not supported when **no supplementary-service sip refer/move-temporary** is configured.

Before You Begin

- Cisco Unified CME 8.6 or a later version.
- The **mode cme** command is configured under voice register global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **camera**
5. **video**
6. **create profile**
7. **exit**
8. **voice register pool** *pool tag*
9. **id mac** *address*
10. **camera**
11. **video**
12. **exit**
13. **voice register template** *template-tag*
14. **camera**
15. **video**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)#voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**camera** **Example:** `Router(config-register-global)#camera`	Enables the **camera** command under voice register global configuration mode.
Step 5	**video** **Example:** `Router(config-register-global)#video`	Enables the **video** command under voice register global configuration mode. **Note** Make sure you configure **video** command without configuring the **camera** command so that Cisco Unified SIP phones can switch from phone-based video camera to CUVA. If you configure both **video** and **camera** commands together, you may need to manually remove the USB camera from Cisco Unified SIP phones .
Step 6	**create profile** **Example:** `Router(config-register-global)# create profile`	Generates provisioning files required for SIP phones and writes the file to the location specified with the **tftp-path** command.
Step 7	**exit** **Example:** `Router(config-register-global)#exit`	Exits voice register global configuration mode.
Step 8	**voice register pool** *pool tag* **Example:** `Router(config)#voice register pool 5`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 9	**id mac** *address* **Example:** `Router(config-register-pool)#id mac 0009.A3D4.1234`	Explicitly identifies a locally available individual SIP phone to support a degree of authentication.

	Command or Action	Purpose
Step 10	**camera** **Example:** `Router(config-register-pool)#camera`	Enables the **camera** command under voice register pool configuration mode.
Step 11	**video** **Example:** `Router(config-register-pool)#video`	Enables the **video** command under voice register pool configuration mode.
Step 12	**exit** **Example:** `Router(config-register-pool)#exit`	Exits voice register pool configuration mode.
Step 13	**voice register template** *template-tag* **Example:** `Router(config)voice register template 10`	Enters voice register template configuration mode to define a template of common parameters for SIP phones in Cisco Unified CME. • Range: 1 to 5.
Step 14	**camera** **Example:** `Router(config-register-template)#camera`	Configures the **camera** command under voice register template configuration mode.
Step 15	**video** **Example:** `Router(config-register-template)#video`	Configures the **video** command under voice register template configuration mode.
Step 16	**end** **Example:** `Router(config-register-template)# end`	Returns to privileged EXEC mode.

Examples

The following example shows the **camera** and **video** commands configured in voice register global configuration mode:

```
Router#show run
!
!
!
voice service voip
 allow-connections sip to sip
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
!
!
voice register global
```

```
 mode cme
 bandwidth video tias-modifier 512000 negotiate end-to-end
 max-pool 10
 camera
 video
!
voice register template  10
```

The following example shows the **video** and **camera** commands configured under voice register pool 5. You can also configure both **camera** and**video** commands under voice register template configuration mode.

```
Router#show run
!
!
voice service voip
 allow-connections sip to sip
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
!
!
voice register global
 mode cme
 bandwidth video tias-modifier 512000 negotiate end-to-end
 max-pool 10

!
voice register pool  1
 id mac 1111.1111.1111
!
voice register pool  4
!
voice register pool  5
 logout-profile 58
 id mac 0009.A3D4.1234
 camera
 video
!
```

What to Do Next

To apply the video and camera configuration to your Cisco Unified SIP IP phones, see Apply Video and Camera Configuration to Cisco Unified SIP Phones, on page 997.

Apply Video and Camera Configuration to Cisco Unified SIP Phones

Apply-config is similar to resetting or restarting the phones and allowing the phones to update phone configuration files. Phones only reboot if needed. To apply video configuration to Cisco Unified IP phones 8845, 8865, 8961, 9951, and 9971, perform the following steps:

Before You Begin

Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **apply-config**
5. **exit**
6. **voice register pool** *pool tag*
7. **apply-config**
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 register global** **Example:** `Router(config)#voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**apply-config** **Example:** `Router(config-register-global)#apply-config`	Applies configuration for the Cisco Unified SIP IP phones and restarts all other SIP phones. The **apply-config** command acts as a reset if configured on any other phone type.
Step 5	**exit** **Example:** `Router(cfg-translation-rule)# exit`	Exits voice register global configuration mode.
Step 6	**voice register pool** *pool tag* **Example:** `Router(config)#voice register pool 5`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 7	**apply-config** **Example:** `Router(config-register-pool)#apply-config`	Applies configuration for the Cisco Unified SIP IP phones and restarts all other SIP phones.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows the **apply-config** command configured in voice register pool 5:

```
Router# configure terminal
Router(config)#voice register pool 5
Router(config-register-pool)#apply-config
```

Configure Video Bandwidth Control for SIP to SIP Video Calls

To configure video bandwidth control for SIP to SIP video calls, perform the following steps:

Before You Begin

Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **bandwidth video tias-modifier** *bandwidth value* [**negotiate** *end-to-end*]
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.

	Command or Action	Purpose
Step 3	**voice register global** **Example:** `Router(config)#voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 4	**bandwidth video tias-modifier** *bandwidth value* [**negotiate** *end-to-end*] **Example:** `Router(config-register-global)#bandwidth video tias-modifier 512000 negotiate end-to-end`	Allows to set the maximum video bandwidth bits per second for SIP phones. • *bandwidth value*—Bandwidth value in bits per second. Range: 1 to 99999999. • **negotiate** *end-to-end*—Bandwidth negotiation policy. Negotiates the minimum SIP-line video bandwidth in SDP end-to-end.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Returns to privileged EXEC mode.

Examples

The following example shows the **bandwith video tias-modifier** command configured under voice register global configuration mode:

```
Router#show run
!
!
!
voice service voip
 allow-connections sip to sip
!
!
voice register global
 mode cme
 source-address 10.100.109.10 port 5060
 bandwidth video tias-modifier 512000 negotiate end-to-end
 max-dn 200
 max-pool 42
 create profile sync 0004625832149157
!
voice register pool  1
 id mac 1111.1111.1111
 camera
 video
```

Enable Support for Video Streams Across H.323 Networks

To enable slow connect procedures in Cisco Unified CME for H.323 networks and H.323 video endpoints, perform the following steps:

Restriction Tandberg versions E3.0 and E4.1 and Polycom Release version 7.5.2 are the only H.323 video endpoints supported by Cisco Unified CME.

Before You Begin

For video supplementary services across an H.323 network, H.450 (H.450.2, H.450.3, or H.450.1) standard protocol is required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **call start slow**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode.
Step 4	**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.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-serv-h323)# end`	Returns to privileged EXEC mode.

Enable System-Level Video Capabilities

To enable video capabilities and set video parameters for all video-capable phones associated with a Cisco Unified CME router, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **service phone videoCapability** {**0** | **1**}
5. **video**
6. **maximum bit-rate** *value*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 4	**service phone videoCapability** {**0** | **1**} **Example:** `Router(config-telephony)# service phone videoCapability 1`	Enables or disables video capability parameter for all applicable IP phones associated with a Cisco Unified CME router. • The parameter name is word and case-sensitive. • **0**—Disable (default). • **1**—Enable.
Step 5	**video** **Example:** `Router(config-telephony)# video`	(Optional) Enters video configuration mode. • Required only if you want to modify the maximum value of the video bandwidth for all video-capable phones.
Step 6	**maximum bit-rate** *value* **Example:** `Router(conf-tele-video)# maximum bit-rate 256`	(Optional) Sets the maximum IP phone video bandwidth, in kilobits per second. • *value*—Range: 0 to 10000000. Default: 10000000.
Step 7	**end** **Example:** `Router(conf-tele-video)# end`	Exits to privileged EXEC mode.

Enable Video Capabilities on a Phone

To enable video for video-capable phones associated with a Cisco Unified CME router, perform the following steps for each phone.

Before You Begin

- Video capabilities are enabled at a system level. See Enable System-Level Video Capabilities, on page 1002.
- Use the **show ephone registered** command to identify individual video-capable SCCP phones, by ephone-tag, that are registered in Cisco Unified CME. The following example shows that ephone 1 has video capabilities and ephone 2 is an audio-only phone:

```
Router# show ephone registered

ephone-1 Mac:0011.5C40.75E8 TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 6 + Video
and Server in ver 5
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
IP:10.1.1.6 51833 7970 keepalive 35 max_line 8
button 1: dn 1 number 8003 CH1 IDLE CH2 IDLE

ephone-2 Mac:0006.D74B.113D TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 6 and Server
```

```
 in ver 5
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
IP:10.1.1.4 51123 Telecaster 7960 keepalive 36 max_line 6
button 1: dn 2 number 8004 CH1 IDLE CH2 IDLE
button 2: dn 4 number 8008 CH1 IDLE CH2 IDLE
===========================================
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **video**
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** *phone-tag* **Example:** `Router(config)# ephone 6`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies an ephone during configuration tasks.
Step 4	**video** **Example:** `Router(config-ephone)# video`	Enables video capabilities on the specified ephone.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Exits ephone configuration mode and enters privileged EXEC mode.

Verify Video Support

Use the **show running-config** command to verify the video settings in the configuration.
See the telephony-service portion of the output for commands that configure video support on the Cisco Unified CME.

See the ephone portion of the output for commands that configure video support for a specific ephone.The following example shows the telephony-service portion of the output:

Example:
```
telephony-service
    video eo
      maximum bit-rate 256
     load 7960-7940 P00306000404
     max-ephones 24
     max-dn 24
     ip source-address 10.0.180.130 port 2000
     service phone videoCapability 1
     timeouts interdigit 4
     timeouts ringing 100
     create cnf-files version-stamp Jan 01 2002 00:00:00
     keepalive 60
     max-conferences 4 gain -6
     call-park system redirect
     call-forward pattern .T
     web admin system name cisco password cisco
     web customize load xml.jeff
     dn-webedit
     time-webedit
     transfer-system full-consult
     transfer-pattern .T
```

The following example shows the ephone portion of the output:

```
ephone  6
 video
 mac-address 000F.F7DE.CAA5
 type 7960
 button  1:6
```

Troubleshooting Video Support

For SCCP endpoint troubleshooting, use the following **debug** commands:

- **debug cch323 video—**Enables video debugging trace on the H.323 service-provider interface (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 Unified IP phones.
- **debug ephone register—**Sets registration debugging for Cisco Unified IP phones.
- **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 off-hook.
- **show ephone registered SCCP—**Displays the status of registered ephones.
- **show ephone summary types—**Displays the number of SCCP phones configured along with the number of phones (registered and unregistered) pertaining to each type of phone.
- **show ephone summary brief—**Displays information about the SCCP phones

  .
- **show ephone registered SCCP summary—**Displays information about the unregistered SCCP phones.
- **show ephone unregistered SCCP summary—**Displays information about the unregistered SCCP phones.
- **show voice register pool type summary—**Displays information about all configured SIP phones which includes SIP phones registered or unregistered with CME.
- **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

After enabling video for video-capable phones in Cisco Unified CME, you must generate a new configuration file. See Generate Configuration Files for Phones, on page 388.

Feature Information for Video Support

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

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

Table 86: Feature Information for Video Support

Feature Name	Cisco Unified CME Version	Feature Information
New Phone Support	12.0	Support was added for Cisco IP Phones 8845 and Cisco IP Phone 8865 on Cisco Integrated Services Router Generation 2 (T-Train Release, 15.7(3)M).
New Phone Support	11.7	Support was added for Cisco IP Phones 8845 and Cisco IP Phone 8865 on Cisco 4000 Series Integration Services Router.
SIP Trunk Video Support	7.1	Support was added for video calls between SCCP endpoints across different Cisco Unified CME routers connected through a SIP trunk. H.264 codec support was added.
Video Support	4.0	Video support was introduced.

CHAPTER 37

SSL VPN Client for SCCP IP Phones

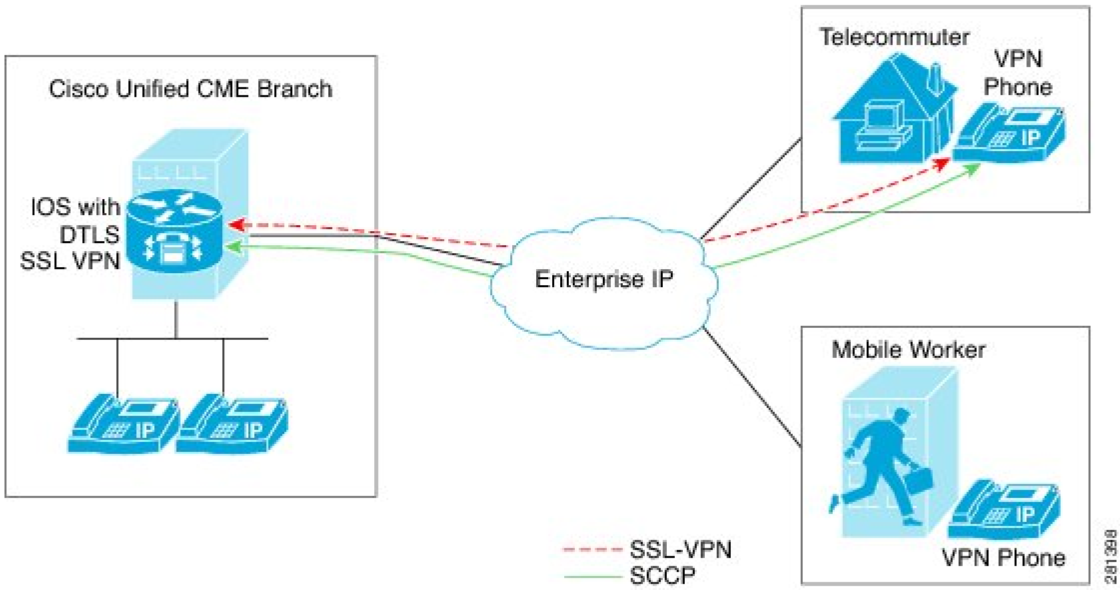
Information About SSL VPN Client

SSL VPN Support on Cisco Unified CME with DTLS

In Communications Manager Express 8.6 and later versions, Cisco Unified SCCP IP phones such as 7945, 7965, and 7975 located outside of the corporate network are able to register to Cisco Unified CME through an SSL VPN connection. The SSL VPN connection is set up between a phone and a VPN headend. The VPN headend can either be an Adaptive Secure Appliance (ASA 5500) or the Datagram Transport Layer Security (DTLS) enabled IOS SSL VPN router, see Figure 37: VPN connection between Cisco Unified IP Phone and

VPN head ends (ASA and DTLS), on page 1010. Support for VPN feature on ASA headend was added in Cisco Unified CME 8.5. For more information, see SSL VPN Client for SCCP IP Phones, on page 1009.

Figure 37: VPN connection between Cisco Unified IP Phone and VPN head ends (ASA and DTLS)



Cisco Unified CME 8.6 uses IOS SSL DTLS as a headend or gateway. To establish a VPN connection between a phone and a VPN head end, the phone must be configured with VPN configuration parameters. The VPN configuration parameters include VPN head end addresses, VPN head end credentials, user or phone ID, and credential policy. These parameters are considered as sensitive information and must be delivered in a secure environment using a signed configuration file or a signed and encrypted configuration file. The phone is required to be provisioned within the corporate network before the phone can be placed outside the corporate network.

After the phone is “staged” in a trusted environment, the phone can be deployed to a location where a VPN head end can be connected. The VPN configuration parameters for the phone dictate the user interface and behavior of the phone.

Phone or Client Authentication

Phone authentication is required to verify that the remote phone trying to register with Cisco Unified CME via, VPN DTLS is a legitimate phone. Phone or client authentication can be done with the following types of authentication:

1. Username and Password Authentication.
2. Certificate-based authentication (where the phone's authentication is done using the LSC or MIC certificate on the phone). The certificated-based authentication consists of two levels:
   - Certificate only Authentication - Where only the LSC of the phone is used (the user is not required to enter a username or password on the phone.)
   - Certification with AAA or two-factor - Where the LSC of the phone and username and password combination is used to authenticate phone. Two-factor authentication can be performed with or

without the username prefill. (With the username prefilled, the phone does not ask for a username and a username is picked up depending on the configuration under the relevant trustpoint.)

Note We recommend using LSC for certificate authentication. Use of MIC for certificate authentication is not recommended. We also recommend configuring ephone in “authenticated” (not encrypted) security mode when doing certificate authentication. More information on certificate-only authentication and two-factor authentication is available at the following location: https://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1465191.

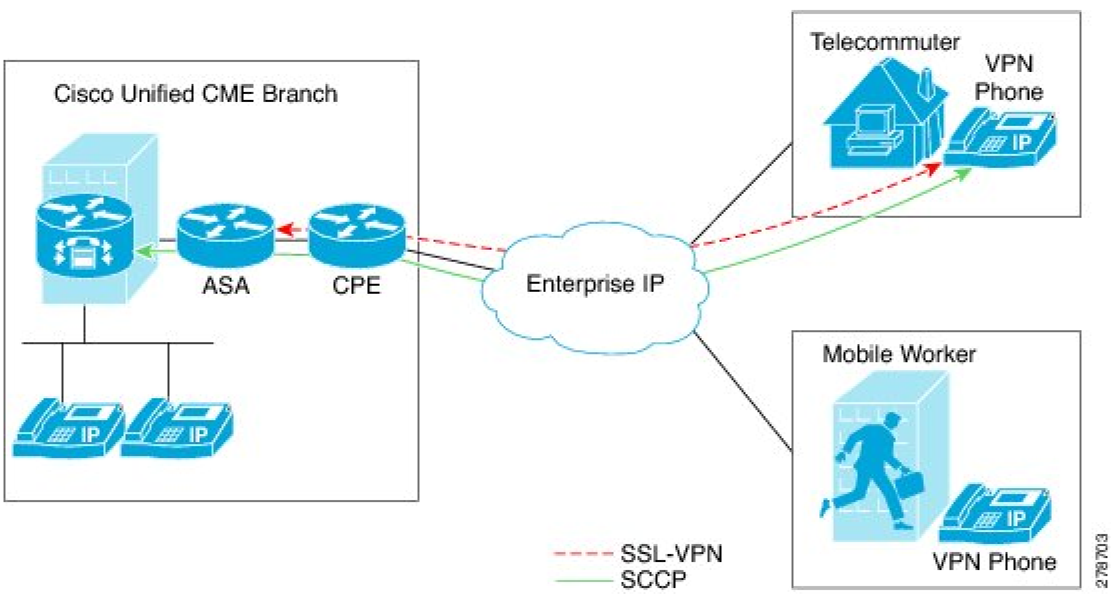
You can set up Cisco Unified CME with an encrypted mode, but encrypted SCCP phone has limited media call-flow support. Using a phone with authenticated mode does not have any media-related call-flow limitations.

SSL VPN Client Support on SCCP IP Phones

Cisco Unified CME 8.5 and later versions support Secure Sockets Layer (SSL) Virtual Private Network (VPN) on SCCP IP phones such as 7945, 7965, and 7975.

In Cisco Unified CME 8.5, SCCP IP phones outside of the corporate network can register with the Cisco Unified CME 8.5 through a VPN connection as shown in Figure 38: Connection between a phone and a VPN head end, on page 1011.

Figure 38: Connection between a phone and a VPN head end



An SSL VPN provides secure communication mechanism for data and other information transmitted between two endpoints. The VPN connection is set up between a SCCP IP phone and a VPN head end or VPN gateway. Cisco Unified CME 8.5 uses an Adaptive Security Appliances (ASA model 55x0) as a VPN head end or gateway.

To establish a VPN connection between a phone and a VPN gateway, the phone is required to be configured with VPN configuration parameters such as VPN gateway addresses, VPN head end credentials, user or phone ID, and credential policy. These parameters contain sensitive information and should be delivered in a secure environment using a signed configuration file or a signed and encrypted configuration file. The phone is required to be provisioned within the corporate network before the phone is placed outside the corporate network.

After the phone is provisioned in a trusted secure environment, the phone can be connected to Cisco Unified CME from any location, from where VPN head end can be reached. The VPN configuration parameters for the phone control the user interface and behavior of the phone. For more information on configuring the SSL VPN feature on SCCP IP phones, see Configure ASA (Gateway) as VPN Headend, on page 1021.

You need to generate a trustpoint with exportable keys and use that as SAST1. For more information about CME System Administrator Security Token.

Configure SSL VPN Client

Configure SSL VPN Client with ASA as VPN Headend

To configure the SSL VPN feature on SCCP IP phones, follow these steps in the order in which they are presented here:

1. Basic Configuration on Cisco Unified CME, on page 1013
2. Configure Cisco Unified CME as CA Server, on page 1018
3. Verify Phone Registration and Phone Load, on page 1020
4. Configure ASA (Gateway) as VPN Headend, on page 1021
5. Configure VPN Group and Profile on Cisco Unified CME, on page 1024
6. Associate VPN Group and Profile to SCCP IP Phone, on page 1026
7. Configure Alternate TFTP Address on Phone, on page 1030
8. Register Phone from a Remote Location, on page 1031

Prerequisites

- Cisco Unified CME 8.5 or later versions.
- Securityk9 license for ISR-G2 platforms.
- Cisco Unified SCCP IP phones 7942, 7945, 7962, 7965, and 7975 with phone image 9.0 or later.
- ASA 5500 series router with image asa828-7-k8.bin or higher.
- The package anyconnect-win-2.4.1012-k9.pkg is required for configuring the SSLVPN feature but would not be downloaded to the phone.
- You must request the appropriate ASA licenses (AnyConnect for Cisco VPN Phone) to be installed on an ASA in order to allow the VPN client to connect. Go to: `www.cisco.com/go/license` and enter the PAK and the new activation key will be e-mailed back to you.

Note A compatible Adaptive Security Device Manager (ASDM) Image is required if configuring through ASDM.

Basic Configuration on Cisco Unified CME

The following steps are basic Cisco Unified configuration allowing the SSL VPN feature to be built on:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *ip-address* [*mask* | *prefix-length*]
5. **option 150 ip** *ip-address*
6. **default-router** *ip-address*
7. **exit**
8. **telephony-service**
9. **max-ephones** *max-phones*
10. **max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**]
11. **ip source-address** *ip-address* **port** *port* [**any-match** | **strict-match**]
12. **cnf-file**{**perphone**}
13. **load** [*phone-type firmware-file*]
14. **no shutdown**
15. **exit**
16. **ephone-dn** *dn-tag* [dual-line]
17. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
18. **ephone** *phone-tag*
19. **description** *string*
20. **device-security-mode**{**authenticated** | **none** | **encrypted**}
21. **mac-address** *mac-address*
22. **type** phone-type [addon 1 module-type [2 module-type]]
23. **button** *button-number* {separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]
24. **exit**
25. **telephony-service**
26. **create cnf-files**
27. **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	**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. **Note** If you have already configured DHCP IP Address Pool, then skip Step 2 to Step 7 and continue from Step 8.
Step 4	**network** *ip-address* [*mask* | *prefix-length*] **Example:** `Router(config-dhcp)#network 192.168.11.0 255.255.255.0`	Specifies the IP address of the DHCP address pool to be configured.
Step 5	**option 150 ip** *ip-address* **Example:** `Router(config-dhcp)# option 150 ip 192.168.11.1`	Specifies the TFTP server address from which the Cisco Unified IP phone downloads the image configuration file. • This is your Cisco Unified CME router's address.
Step 6	**default-router** *ip-address* **Example:** `Router(config-dhcp)# default router 192.168.11.1`	(Optional) Specifies the router that the IP phones will use to send or receive IP traffic that is external to their local subnet. • If the Cisco Unified CME router is the only router on the network, this address should be the Cisco Unified CME IP source address. This command can be omitted if IP phones need to send or receive IP traffic only to or from devices on their local subnet. • The IP address that you specify for default router will be used by the IP phones for fallback purposes. If the Cisco Unified CME IP source address becomes unreachable, IP phones will attempt to register to the address specified in this command.
Step 7	**exit** **Example:** `Router(config-dhcp)# end`	Exits DHCP pool configuration mode.

	Command or Action	Purpose
Step 8	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 9	**max-ephones** *max-phones* **Example:** `Router(config-telephony)# max-ephones 24`	Sets the maximum number of phones that can register to Cisco Unified CME. • Maximum number is platform and version-specific. Type ? for range. • In Cisco Unified CME 7.0/4.3 and later versions, the maximum number of phones that can register is different than the maximum number of phones that can be configured. The maximum number of phones that can be configured is 1000. • In versions earlier than Cisco Unified CME 7.0/4.3, this command restricted the number of phones that could be configured on the router.
Step 10	**max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**] **Example:** `Router(config-telephony)# max-dn 24 no-reg primary`	Limits number of directory numbers to be supported by this router. • Maximum number is platform and version-specific. Type ? for value.
Step 11	**ip source-address** *ip-address* **port** *port* [**any-match** | **strict-match**] **Example:** `Router(config-telephony)# ip source-address 192.168.11.1 port 2000`	Identifies the IP address and port number that the Cisco Unified CME router uses for IP phone registration. • **port** *port*—(Optional) TCP/IP port number to use for SCCP. Range is 2000 to 9999. Default is 2000. • **any-match**—(Optional) Disables strict IP address checking for registration. This is the default. • **strict-match**—(Optional)) Instructs the router to reject IP phone registration attempts if the IP server address used by the phone does not exactly match the source address.
Step 12	**cnf-file**{**perphone**} **Example:** `Router(config-telephony)#xnf-file perphone`	Specifies that system generate a separate configuration XML file for each IP phone. • Separate configuration files for each endpoint are required for security. **Note** You must configure the cnf-file (perphone) command to generate a separate XML file for each phone.

	Command or Action	Purpose
Step 13	**load** [*phone-type firmware-file*] **Example:** `Router(config-telephony)# load 7965 SCCP45.9-0-1TD1-36S.loads`	Associates a phone type with a phone firmware file. You must use the complete filename, including the file suffix, for phone firmware versions later than version 9.0 for all phone types load 7965 SCCP45.9-0-1TD1-36S
Step 14	**no shutdown** **Example:** `Router(config-telephony)# no shutdown`	Allows to enable SCCP service listening socket.
Step 15	**exit** **Example:** `Router(config-telephony)# end`	Exits telephony-service configuration mode.
Step 16	**ephone-dn** *dn-tag* [dual-line] **Example:** `Router(config)# ephone-dn 1`	Enters ephone dn configuration mode to define a directory number for an IP phone, intercom line, voice port, or a message-waiting indicator (MWI). • *dn-tag*—identifies a particular directory number during configuration tasks. Range is 1 to the maximum number of directory numbers allowed on the router platform. Type ? to display the range.
Step 17	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 1001`	Associates an extension number with this directory number. • *number*—String of up to 16 digits that represents an extension or E.164 telephone number.
Step 18	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode to set ephone specific parameters. • *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type ? to display range.
Step 19	**description** *string* **Example:** `Router(config-ephone)description SSL VPN Remote Phone`	Ephone descriptions for network management systems using an eXtensible Markup Language (XML) query. • *string*—Allows for a maximum of 128 characters, including spaces. There are no character restrictions.
Step 20	**device-security-mode**{**authenticated** | **none** | **encrypted**} **Example:** `Router(config-ephone)# device-security-mode none`	Allows to set the security mode for SCCP signaling for devices communicating with the Cisco Unified CME router globally or per ephone.

	Command or Action	Purpose
		• authenticated— SCCP signaling between a device and Cisco Unified CME through the secure TLS connection on TCP port 2443. • none— SCCP signaling is not secure. • encrypted — SCCP signaling between a device and Cisco Unified CME through the secure TLS connection on TCP port 2443, and the media uses Secure Real-Time Transport Protocol (SRTP).
Step 21	**mac-address** *mac-address* **Example:** `Router(config-ephone)# mac-address 0022.555e.00f1`	Associates the MAC address of a Cisco IP phone with an ephone configuration in a Cisco Unified CME system • *mac-address*—identifying MAC address of an IP phone, which is found on a sticker located on the bottom of the phone.
Step 22	**type** phone-type [addon 1 module-type [2 module-type]] **Example:** `Router(config-ephone)# type 7965`	Specifies the type of phone. • Cisco Unified CME 4.0 and later versions—The only types to which you can apply an add-on module are 7960, 7961, 7961GE, and 7970.
Step 23	**button** *button-number* {separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...] **Example:** `Router(config-ephone)# button 1:1`	Associates a button number and line characteristics with an ephone-dn. Maximum number of buttons is determined by phone type.
Step 24	**exit** **Example:** `Router(config-ephone)#exit`	Exits ephone configuration mode.
Step 25	**telephony-service** **Example:** `Router(config)telephony-service`	Enters telephony-service configuration mode.
Step 26	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds XML configuration files required for SCCP phones.
Step 27	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Cisco Unified CME as CA Server

The basic configuration on the CA server ensures IP connectivity, Network Time Protocol (NTP), time synchronization which are necessary for enabling the SSL VPN feature.

Though this section describes configuring CA server on the CME to provide certificate signing for both CME and ASA, in real world deployments third party CA is often used. The basic requirement is that CME and ASA each has an identity certificate signed by the third party CA, and both CME and ASA share the same CA certificate. That is, each device has a trustpoint containing the same CA certificate as well as an identity certificate signed by the same CA.

To configure the CA server, follow these steps:

Step 1 Configure IP Address, NTP and HTTP Server on your Cisco Unified CME router:

Example:

```
Router(config)# Interface GigabitEthernet0/0
Router(config-if)# no ip address
Router(config-if)# interface GigabitEthernet0/0.10
Router(config-subif)# description DATA VLAN
Router(config-subif)# encapsulation dot1Q 10 native
Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config)# interface GigabitEthernet0/0.11
Router(config-subif)# description VOICE VLAN
Router(config-subif)# encapsulation dot1Q 11
Router(config-subif)# ip address 192.168.11.1 255.255.255.0

Router(config)# interface GigabitEthernet0/1
Router(config-if)# description INTERFACE CONNECTED TO ASA
Router(config-if)# ip address 192.168.20.1 255.255.255.0

Router(config)# ! Default router is ASA Inside Interface
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.20.254
Router(config)# clock timezone PST -8
Router(config)# clock summer-time PST recurring

Router# ! Set clock to current time
Router# clock set 10:10:00 15 oct 2010

Router(config)# ntp source GigabitEthernet0/1
Router(config)# ntp master 2

Router(config)# ip http server
Router(config)# ip domain-name cisco.com
```

Note NTP synchronization will fail if you do not set the clock manually to match the time on Cisco Unified CME router.

Step 2 Configure Cisco Unified CME as CA Server. Both CME and ASA will enroll a certificate from the CA Server. The following sample configuration shows Cisco Unified CME being configured as the CA Server:

Example:

```
Router(config)# crypto pki server cme_root
Router(config)# database level complete
Router(cs-server)# database url nvram:
```

```
Router(cs-server)# grant auto
Router(cs-server)# lifetime certificate 7305
Router(cs-server)# lifetime ca-certificate 7305
Router(cs-server)# exit

Router(config)# crypto pki trustpoint cme_root
Router(ca-trustpoint)# enrollment url http://192.168.20.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair cme_root
Router(cs-server)# exit

Router(config)# crypto pki server cme_root
Router(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: *****
Re-enter password: ****
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
Mar 10 16:44:00.576: %SSH-5-ENABLED: SSH 1.99 has been enabled% Exporting Certificate
Server signing certificate and keys...
% Certificate Server enabled.
Router(cs-server)#
Mar 10 16:44:41.812: %PKI-6-CS_ENABLED: Certificate server now enabled.
```

Step 3 Create a second trustpoint, then authenticate the trustpoint and enroll it with CA.

Example:

```
Router(config)# crypto pki trustpoint cme_cert
Router(ca-trustpoint)# enrollment url http://192.168.20.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit

Router(config)# crypto pki authenticate cme_cert
Certificate has the following attributes:
Fingerprint MD5: 995C157D AABB8EE2 494E7B35 00A75A88
Fingerprint SHA1: F934871E 7E2934B1 1C0B4C9A A32B7316 18A5858F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Router(config)# crypto pki enroll cme_cert
%
% 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:
Jan 20 16:03:24.833: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:
% The subject name in the certificate will include: CME1.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose cme_cert' command will show the fingerprint.
! Verify Certificates
```

Verify Certificates (Optional)

Use the **show crypto pki certificates** command on your Cisco Unified CME router to verify the certificates.

```
Router# sh crypto pki certificates
Certificate
Status: Available
Certificate Serial Number (hex): 07
Certificate Usage: General Purpose
Issuer:
cn=cme_root
```

```
Subject:
Name: CME1.cisco.com
hostname=CME1.cisco.com
Validity Date:
start date: 15:32:23 PST Apr 1 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cisco2
Storage: nvram:cme_root#7.cer

Certificate
Status: Available
Certificate Serial Number (hex): 06
Certificate Usage: General Purpose
Issuer:
cn=cme_root
Subject:
Name: CME1.cisco.com
hostname=CME1.cisco.com
Validity Date:
start date: 15:30:11 PST Apr 1 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cisco1
Storage: nvram:cme_root#6.cer

Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=cme_root
Subject:
Name: CME1.cisco.com
hostname=CME1.cisco.com
Validity Date:
start date: 08:47:42 PST Mar 10 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cme_cert
Storage: nvram:cme_root#2.cer

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=cme_root
Subject:
cn=cme_root
Validity Date:
start date: 08:44:00 PST Mar 10 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cisco2 cisco1 cme_cert cme_root
Storage: nvram:cme_root#1CA.cer
```

Verify Phone Registration and Phone Load

Step 1 Use the **show ephone** command to verify the phone registration details.

Example:

```
Router# show ephone
```

```
ephone-1[0] Mac:0022.555E.00F1 TCP socket:[2] activeLine:0 whisperLine:0 REGISTERED in SCCP ver 19/17
 max_streams=5 mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0 caps:9
IP:192.168.11.4 * 49269 7965 keepalive 0 max_line 6 available_line 6
button 1: cw:1 ccw:(0 0) dn 1 number 1001 CH1   IDLE CH2   IDLE
Preferred Codec: g711ulaw
Lpcor Type: none
```

Note Make sure the phone has the right phone firmware and verify if the phone registers locally with Cisco Unified CME.

Step 2 Use the **show ephone phone load** command to verify phone load.

Example:

```
Router# show ephone phoneload

DeviceName        CurrentPhoneload       PreviousPhoneload LastReset

SEP0016C7EF9B13    9.0(1TD1.36S)          9.0(1TD1.36S) UCM-closed-TCP
```

Configure ASA (Gateway) as VPN Headend

In this section ASA will be configured to authenticate and enroll a certificate from CME CA server. The fingerprint of the CA certificate will be the same as the CME root certificate, so that the phone can authenticate the certificates sent from ASA during TLS negotiation against the hash it has in store.

Step 1 Configure Interfaces, IP Routing, and NTP.

Example:

```
ciscoasa(config)# Interface Ethernet0/1
ciscoasa(config-if)# nameif Inside
ciscoasa(config-if)# description INTERFACE CONNECTED TO CUCME
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.20.254 255.255.255.0

ciscoasa(config)# interface Ethernet 0/0
ciscoasa(config-if)# description INTERFACE CONNECTED TO WAN
ciscoasa(config-if)# nameif Outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 9.10.60.254 255.255.255.0
ciscoasa(config)# router ospf 100
ciscoasa(config-router)# network 9.10.60.0 255.255.255.0 area 1

ciscoasa(config-if)# ntp server 192.168.20.1
```

Step 2 Create Trustpoint on ASA and obtain CME (CA) Certificate.

Example:

```
ciscoasa(config)# crypto key generate rsa label cmeasa
ciscoasa(config)# crypto ca trustpoint asatrust
ciscoasa(config)# ! Enrollment URL = CA Server = CUCME
ciscoasa(config-ca-trustpoint)# enrollment url http://192.168.20.1:80
ciscoasa(config-ca-trustpoint)# subject-name cn=cmeasa.cisco.com
```

```
ciscoasa(config-ca-trustpoint)# crl nocheck
ciscoasa(config-ca-trustpoint)# keypair cmeasa

ciscoasa (config)# crypto ca authenticate asatrust
INFO: Certificate has the following attributes:
Fingerprint: 27d00cdf 1144c8b9 90621472 786da0cf
Do you accept this certificate? [yes/no]: yes
! Enroll the Trustpoint
ciscoasa(config)# crypto ca enroll asatrust
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: ********
Re-enter password: ********
% The subject name in the certificate will be: cn=cmeasa.cisco.com
% The fully-qualified domain name in the certificate will be: ciscoasa.cisco.com
% Include the device serial number in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ciscoasa(config)# The certificate has been granted by CA!
ciscoasa# show crypto ca certificates
```

Step 3 Verify Certificates (optional)

Use the **show crypto ca certificate** command on your ASA router to verify the certificates.

Example:

```
ciscoasa# show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 03
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
cn=cme_root
Subject Name:
hostname=ciscoasa.cisco.com
cn=cmeasa.cisco.com
Validity Date:
start date: 09:04:40 PST Mar 10 2010
end date: 08:44:00 PST Mar 10 2030
Associated Trustpoints: asatrust

CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Public Key Type: RSA (1024 bits)
Issuer Name:
cn=cme_root
Subject Name:
cn=cme_root
Validity Date:
start date: 08:44:00 PST Mar 10 2010
end date: 08:44:00 PST Mar 10 2030
Associated Trustpoints: asatrust
```

Step 4 Configure SSL Parameters.

Example:

```
ciscoasa(config)# ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 null-sha1
ciscoasa(config)#
ciscoasa(config)# ssl trust-point asatrust
ciscoasa(config)# ssl trust-point asatrust inside
```

```
ciscoasa(config)# ssl trust-point asatrust outside
ciscoasa(config)# no ssl certificate-authentication interface outside port 443
ciscoasa(config)# ssl certificate-authentication interface inside port 443
```

Step 5 Configure local IP address pool.

Example:

```
ciscoasa(config)# ip local pool SSLVPNphone_pool 192.168.20.50-192.168.20.70 mask
255.255.255.0
```

Step 6 Configure Access List to prevent NAT traffic via VPN.

Example:

```
ciscoasa(config)# access-list no_nat_to_vpn extended permit ip any 9.10.60.0 255.255.255.0
ciscoasa(config)# ! 9.10.60.0/24 is the Outside subnet
ciscoasa(config)# nat (inside) 0 access-list no_nat_to_vpn
```

Step 7 Configure VPN. Follow this link for information on configuring VPN: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/svc.html.

Example:

```
ciscoasa(config-webvpn)# enable inside
INFO: WebVPN and DTLS are enabled on 'Inside'.
ciscoasa(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'Outside'.
ciscoasa(config-webvpn)# svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
ciscoasa(config-webvpn)# svc enable
ciscoasa(config-webvpn)# group-policy SSLVPNphone internal
ciscoasa(config)# group-policy SSLVPNphone attribute
ciscoasa(config-group-policy)# banner none
ciscoasa(config-group-policy)# vpn-simultaneous-logins 10
ciscoasa(config-group-policy)# vpn-idle-timeout none
ciscoasa(config-group-policy)# vpn-session-timeout none
ciscoasa(config-group-policy)# vpn-tunnel-protocol svc webvpn
ciscoasa(config-group-policy)# address-pools value SSLVPNphone_pool
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# svc dtls enable
ciscoasa(config-group-webvpn)# svc keepalive 120
ciscoasa(config-group-webvpn)# svc ask none
ciscoasa(config-group-webvpn)#
```

Step 8 Configure SSL VPN tunnel. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/vpngrp.html.

Example:

```
ciscoasa(config)# tunnel-group SSLVPN_tunnel type remote-access
ciscoasa(config)# tunnel-group SSLVPN_tunnel general-attributes
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)# address-pool SSLVPNphone_pool
ciscoasa(config-tunnel-general)# default-group-policy SSLVPNphone
ciscoasa(config-tunnel-general)# tunnel-group SSLVPN_tunnel webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://9.10.60.254/SSLVPNphone enable
```

Step 9 Enable static route to Cisco Unified CME voice VLAN. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/route_static.html.

Example:
```
ciscoasa(config)# route Inside 192.168.11.0 255.255.255.0 192.168.20.254 1
```

Step 10 Configure the ASA local database for users. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_aaa.html#wpmkr108.

Example:

```
ciscoasa(config)# username anyone password cisco
ciscoasa(config)# ! These credentials will be entered on the phone to log in.
ciscoasa(config)# username anyone attributes
ciscoasa(config-username)# vpn-group-policy SSLVPNphone
ciscoasa(config-username)# vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# svc dtls enable
ciscoasa(config-username-webvpn)# svc ask none
```

Step 11 Enable Inter-ASA media traffic.

Example:

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config)# same-security-traffic permit intra-interface
```

Configure VPN Group and Profile on Cisco Unified CME

In this section a VPN-group is configured which dictates the VPN gateway IP address, certificate hash algorithm and certificate trustpoint for phones. This information will be added to phone configuration later. To configure VPN group and profile on Cisco Unified CME, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **vpn-group** *tag*
5. **vpn-gateway** [*number* | **url**]
6. **vpn-trustpoint** {[*number* [**raw** | **trustpoint**]}
7. **vpn-hash-algorithm** *sha-1*
8. **exit**
9. **vpn-profile** *tag*
10. **host-id-check** [**enable** | **disable**]
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)#voice service voip`	Enters voice over IP configuration mode.
Step 4	**vpn-group** *tag* **Example:** `Router (conf-voi-serv)#vpn-group 1`	Enters vpn-group mode under voice over IP configuration mode. • *tag*—vpn-group tag. Range: 1 or 2.
Step 5	**vpn-gateway** [*number* | **url**] **Example:** `Router(conf-vpn-group)#vpn-gateway 1 https://9.10.60.254/SSLVPNphone`	Allows you to define gateway url for vpn. • *number*—number—Number of gateways that can be defined as a vpn-gateway. Range is from 1 to 3. • *url*—VPN-gateway url. SSLVPNphone is the VPN group policy configured on ASA.
Step 6	**vpn-trustpoint** {[*number* [**raw** | **trustpoint**]} **Example:** `Router(conf-vpn-group)#vpn-trustpoint ?vpn-trustpoint 1 trustpoint cme_cert root`	Allows you to enter a vpn-gateway trustpoint. • **number**—Number of trustpoints allowed. Range:1 to 10. • **raw—**allows you to enter vpn-gateway trustpoint in raw format. • **trustpoint—**allows you to enter VPN Gateway trustpoint as created in IOS format. • **root –** Since the CME root certificate has the same hash as ASA's CA certificate, therefore the "root" clause is configured to select the root certificate instead of leaf certificate.
Step 7	**vpn-hash-algorithm** *sha-1* **Example:** `Router(conf-vpn-group)#vpn-hash-algorithm sha-1`	Allows you to enter vpn hash encryption for the trustpoints. • *sha-1*—Encryption algorithm.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(conf-vpn-group)#exit`	Exits VPN-group configuration mode.
Step 9	**vpn-profile** *tag* **Example:** `Router (conf-voi-serv)#vpn-profile 1`	Enters VPN-profile configuration mode. *tag*—VPN-profile tag number. Range: 1-6.
Step 10	**host-id-check** [**enable** | **disable**] **Example:** `Router(conf-vpn-profile)#host-id-check disable`	Allows you to configure host id check option in VPN-profile. • disable— Disable host ID check option. • enable— Enable host ID check option. Default is Enable.
Step 11	**end** **Example:** `Router(conf-vpn-profile)#end`	Exits to privileged EXEC mode.

Associate VPN Group and Profile to SCCP IP Phone

To associate VPN group and profile to SCCP IP phones, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **cnf-file perphone**
5. **ephone** *phone-tag*
6. **device-security-mode** {authenticated | none | encrypted}
7. **mac-address** [mac-address]
8. **type** *phone-type* **addon 1** *[module-type* [**2** *module-type*]]
9. **vpn-group** *tag*
10. **vpn-profile** *tag*
11. **button** *button-number{separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]*
12. **exit**
13. **telephony-service**
14. **create cnf-file**
15. **exit**
16. **ephone** *phone-tag*
17. **reset**
18. **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	**telephony-service** **Example:** `Router#(config)telephony-service`	Enters telephony-service configuration mode.
Step 4	**cnf-file perphone** **Example:** `Router(config-telephony)# create cnf-files`	Builds the XML configuration files required for IP phones.

	Command or Action	Purpose
Step 5	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode to set phone-specific parameters for an SCCP phone. • *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range
Step 6	**device-security-mode** {authenticated | none | encrypted} **Example:** `Router(config-telephony)# device-security-mode none`	Enables security mode for endpoints. • authenticated—Instructs device to establish a TLS connection with no encryption. There is no Secure Real-Time Transport Protocol (SRTP) in the media path. • none—SCCP signaling is not secure. This is the default. • encrypted—Instructs device to establish an encrypted TLS connection to secure media path using SRTP. • The value set for this command in ephone configuration mode has priority over the value set in telephony-service configuration mode.
Step 7	**mac-address** [mac-address] **Example:** `Router(config-ephone)#mac-address 0022.555e.00f1`	Specifies the MAC address of the IP phone that is being configured
Step 8	**type** *phone-type* **addon 1** *[module-type* [**2** *module-type*]] **Example:** `Router(config-ephone)# type 7965`	Specifies the type of phone. • Cisco Unified CME 4.0 and later versions—The only types to which you can apply an add-on module are 7960, 7961, 7961GE, and 7970. • Cisco CME 3.4 and earlier versions—The only type to which you can apply an add-on module is 7960.
Step 9	**vpn-group** *tag* **Example:** `Router (config-ephone)# vpn-group 1`	Enters vpn-group mode under voice over IP configuration mode. • tag—vpn-group tag. Range: 1 or 2.
Step 10	**vpn-profile** *tag* **Example:** `Router (config-ephone)#vpn-profile 1`	Enters VPN-profile configuration mode. • tag—VPN-profile tag number. Range: 1-6.

	Command or Action	Purpose
Step 11	**button** *button-number{separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]* **Example:** `Router(config-ephone)# button 1:5`	Associates a button number and line characteristics with an ephone-dn. Maximum number of buttons is determined by phone type.
Step 12	**exit** **Example:** `Router(config-ephone)exit`	Exits ephone configuration mode.
Step 13	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 14	**create cnf-file** **Example:** `Router(config-telephony)# create cnf-files`	Builds the XML configuration files required for IP phones. It is recommended to first clear the existing config files using "no create cnf-files" and then create again.
Step 15	**exit** **Example:** `Router(Config-telephony)exit`	Exits telephony service configuration mode.
Step 16	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 17	**reset** **Example:** `Router(config-ephone)# reset`	Performs a complete reboot of the individual SCCP phone being configured.
Step 18	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Configure Alternate TFTP Address on Phone

Step 1 From the phone, go to:

Example:

```
Settings > Network Configuration > IPv4 Configuration > Alternate TFTP

Press **# to unlock
Select YES

If the phone is already registered, “TFTP Server 1” will already be populated. Otherwise, enter the
CUCME address as the alternate TFTP Server 1.
```

Step 2 Save the phone configuration.

Step 3 Verify if the VPN is enabled from the phone.

Example:

```
Settings > Security Configuration > VPN

When you press “Enable” from this menu, it should prompt for username and password.
```

Step 4 From the phone, go to:

Example:

```
Settings > Network Configuration > IPv4 Configuration > Alternate TFTP

Press **# to unlock and select YES.

If the phone is already registered, “TFTP Server 1” will already be populated. Otherwise, enter the
CUCME address as the alternate TFTP Server 1.
```

Step 5 Save the configuration.

Step 6 Connect the phone to the network from home or a remote location.

Example:

```
Settings > Security Settings > VPN Configurations?

Enable VPN
Enter Username and Password. Phone will register with CUCME.
```

Register Phone from a Remote Location

To register a Cisco Unified IP phone from a remote location, follow these steps:

Step 1 Connect the phone to the network from a home or remote location. Phone receives DHCP.

Step 2 Select **Settings** from the phone menu and go to **Security Settings**.

Step 3 Select **VPN Configurations**. and then select **Enable VPN**.

Step 4 Enter your username and password. Your phone will now register with Cisco Unified CME.

Configure SSL VPN Client with DTLS on Cisco Unified CME as VPN Headend

Before you begin, make sure you have configured the basic SSL VPN configuration on Cisco Unified CME (see Basic Configuration on Cisco Unified CME, on page 1013).

To configure the SSL VPN client with DTLS on SCCP IP phones, follow these steps in the order in which they are presented here:

- Set Up the Clock, Hostname, and Domain Name, on page 1032
- Configure Trustpoint and Enroll with the Certificates, on page 1033
- Configure VPN Gateway, on page 1033
- Configure User Database, on page 1033
- Configure Virtual Context, on page 1034
- Configure Group Policy, on page 1034
- Verify the IOS SSL VPN Connection, on page 1035
- Configure Cisco Unified SCCP IP Phones for SSL VPN, on page 1035
- Configuration on Cisco Unified SCCP IP Phone, on page 1036
- Configure SSL VPN on Cisco Unified CME, on page 1036

Note Depending upon the type of authentication you choose to configure, configuration steps 3 to step 11 may vary a little from the way they are documented in this section.

Set Up the Clock, Hostname, and Domain Name

The clock, hostname, and domain name must be set up.

Step 1 The following example shows the hostname and domain name configured:

Example:

```
hostname Router2811
ip domain name cisco.com

Interfaces on the Router_2811:

interface FastEthernet0/0
ip address 1.5.37.13 255.255.0.0
duplex auto
speed auto

interface FastEthernet0/1
ip address 30.0.0.1 255.255.255.0
duplex auto
speed auto
```

Step 2 Show clock on IOS:

Example:

```
Router# show clock
*10:07:57.109 pacific Thu Oct 7 2010
```

a) Set clock directly:

Example:

```
Router# clock set 9:53:0 Oct 7 2010

Set time zone (Pacific Standard Time)
Router# configure terminal
Router(config)# clock timezone pst -8

(optional)
Set summer-time
Router# configure terminal

Router(config)# clock summer-time pst recurring
```

OR

```
Router(config)# clock summer-time pst date apr 11 2010 12:00 nov 11 2010 12:00
```

b) Set clock using NTP:

Example:

```
Router(config)# ntp server 192.18.2.1
Router(config)# ntp master 2
```

Configure Trustpoint and Enroll with the Certificates

To configure a trustpoint and enroll with the certificate server, see Configure Cisco Unified CME as CA Server, on page 1018. You can also use the default self-signed certificate generated by the webvpn. This default **trustpoint** is generated when the webvpn gateway **gateway name** command is entered for the first time.

Note The DTLS in IOS SSL VPN uses the child certificate during SSL authentication, therefore, you must select the “leaf” option when configuring the “vpn-trustpoint”.

Configure VPN Gateway

The WebVPN gateway uses a default trustpoint name of SSL VPN.

When entering “webvpn gateway <name>”, a self-signed certificate is generated. The IP address must be a public IP address configured on an interface or loopback interface on the WebVPN gateway. The following example shows a public IP address configured on the WebVPN gateway:

```
Router(config)# webvpn gateway sslvpn_gw
Router(config-webvpn-gateway)# ip address 1.5.37.13 port 443
Router(config-webvpn-gateway)# ssl encryption 3des-sha1 aes-sha1
Router(config-webvpn-gateway)# ssl trustpoint cme_cert
Router(config-webvpn-gateway)# inservice
```

Note We recommend using Cisco Unfied CME generated trustpoint rather than webvpn self generated trustpoint.

Configure User Database

User database can be either locally configured on CME, or remotely from Radius server.

Step 1 Configure the local database:

Example:

```
Router(config)# aaa new-model
username anyone password 0 cisco
aaa authentication login default local
```

Step 2 Configure a remote AAA Radius server for authentication:

Example:

```
Router(config)# aaa new-model
aaa authentication login default group radius
radius-server host 172.19.159.150 auth-port 1923 acct-port 1924
radius-server key cisco
```

For more information, see http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/aaa.html#wp1062044.

Configure Virtual Context

Users can get access to the virtual context by specifying the “domain name” in the URL when accessing the WebVPN gateway such as: https://1.5.37.13/SSLVPNphone. The following example shows a virtual VPN context configured:

```
Router(config)# webvpn context sslvpn_context
 ssl encryption 3des-sha1 aes-sha1
 ssl authenticate verify all
 gateway sslvpn_gw domain SSLVPNphone
 inservice
```

When **inservice** was entered, the system prompted: **000304: Jan 7 00:30:01.206: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up**

Configure Group Policy

Because the SSL VPN client on phone operates in full-tunnel mode, WebVPN gateway supplies an IP address to each of the clients logged in to the gateway. Configure the following:

```
Router(config)# ip local pool SSLVPNphone_pool 30.0.0.50 30.0.0.70
Router(config)# webvpn context SSLVPNphone
Router(config-webvpn-context)# policy group SSLVPNphone
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)# svc address-pool "SSLVPNphone_pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc default-domain "cisco.com"
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy SSLVPNphone
Router(config-webvpn-context)# no aaa authentication domain local
Router(config-webvpn-context)# gateway sslvpn_gw domain SSLVPNphone
```

If using only username and password authentication, configure:

```
Router(config-webvpn-context)# no authentication certificate
```

If using certificate-based authentication, configure:

```
Router(config-webvpn-context)# authentication certificate

Router(config-webvpn-context)# ca trustpoint cme_cert
Router(config-webvpn-context)# inservice
```

Verify the IOS SSL VPN Connection

On your PC's browser (MS Internet Explorer), connect to https://1.5.37.13/SSLVPN phone and accept the certificate. To login, enter username and password, anyone and cisco. You should be able to see the home page of the IOS SSL VPN.

Step 1 IOS WEBVPN DEBUG:

Example:

```
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states

debug webvpn sdps
debug webvpn aaa (login authentication)

debug webvpn http verbose (for authentication)
debug webvpn webservice verbose
debug webvpn tunnel

debug crypto pki transactions
debug crypto pki validations
debug crypto pki messages
```

From PC browser, connect to IOS (on the 1.5.37.x network) through https://1.5.37.13/SSLVPN phone. The default banner pops up. Enter username and password.

Step 2 Provide the default IP route. For example:

Example:

```
Router (c3745): ip route 30.0.0.0 255.255.255.0 FastEthernet0/
Router (c3745): ip route 10.0.0.0 255.255.255.0 1.5.37.11
```

(Must force this limited route or else it will fail).

Configure Cisco Unified SCCP IP Phones for SSL VPN

Step 1 Phone loads are available for download at Cisco Unified Communications Manager Express Introduction.

Step 2 Choose **Compatibility Information**.

Step 3 Choose appropriate phone load version for your phone.
A generic software download is also available at Product/Technology Support.

Step 4 Choose **Voice and Unified Communications** > **IP Telephony** > **IP Phones**.

Note We recommend downloading phone load version 8.4 before upgrading phone load version 8.3 to phone load version 9.0. Upgrading phone load to 9.0 without upgrading the phone load version to 8.4 will not work.

Step 5 After a hard reset (press # while power up), the *term65.default.loads* can be used to load the rest of the images.

Configuration on Cisco Unified SCCP IP Phone

Step 1 Go to **Settings** > **Security configuration (4)** > **VPN Configuration (8)** .

Step 2 Check the IP address of the VPN concentrator. It should point to the VPN headend.

Step 3 Verify Alt-TFTP (under **Settings** > **Network Configuration** > **IPv4 Configuration**). Set the Alternate TFTP option to "Yes" to manually enter the TFTP server address. The associated IP address is the IP address of Cisco Unified CME.

Step 4 Set the VPN setting to **enable**. The user interface shows, "`Attempting VPN Connection...`".

Step 5 Verify that the VPN connection is established. Go to **Settings** > **Network Configuration** . The "VPN" label shows "`connected`".

Note If you are using phones in secure mode, remember to add the **capf-ip-in-cnf** command under ephone configuration mode.

Configure SSL VPN on Cisco Unified CME

To configure SSL VPN on Cisco Unified CME, see Configure VPN Group and Profile on Cisco Unified CME, on page 1024.

Example:

```
voice service voip
 vpn-group 1
  vpn-gateway 1 https://1.5.37.13/SSLVPNphone
  vpn-trustpoint 1 trustpoint R2811_cert leaf
 vpn-profile 1
  host-id-check disable

crypto pki server R2811_root
 database level complete
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
crypto pki token default removal timeout 0
!
crypto pki trustpoint R2811_root
 enrollment url http://30.0.0.1:80
 revocation-check none
 rsakeypair R2811_root
!
crypto pki trustpoint R2811_cert
 enrollment url http://30.0.0.1:80
 serial-number
 revocation-check none

telephony-service
 cnf-file perphone

ephone 2
```

```
 device-security-mode none
 mac-address 001E.7AC4.DD25
 type 7965
 vpn-group 1
 vpn-profile 1
 button 1:5

telephony-service
 create cnf-files

ephone 2
 reset
```

VPN Phone Redundancy Support for Cisco Unified CME with DTLS

VPN phone supports redundancy with IOS and Cisco Unified CME in two ways:

1. Using two or more vpn-gateway configurations in the same vpn-group.
2. Using Cisco Unified CME redundancy configuration and one or more vpn-gateway configurations. This requires the DTLS and SSL VPN headend IP to stay up, if only one vpn-gateway is used.

Cisco Unified CME redundancy works when you import a trustpoint from primary CME to secondary CME. See http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c5.html#wp1044112. For more information on reduntant Cisco Unified CME, see Redundant Cisco Unified CME Router for SCCP Phones, on page 160.

You need to generate a trustpoint with exportable keys and use that as sast1.

Configuration Examples for SSL VPN Client

Example for Configuring SSL VPN with ASA as VPN Headend

The following example shows how to configure CME using ASA as VPN Headend:

```
Router# show running config
!
!
!
crypto pki server cme_root
 database level complete
 no database archive
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
!
crypto pki trustpoint cme_root
 enrollment url http://10.201.160.201:80
 revocation-check none
 rsakeypair cme_root
!
crypto pki trustpoint cme_cert
 enrollment url http://10.201.160.201:80
 revocation-check none
!
!
!
!
voice service voip
```

```
vpn-group 1
 vpn-gateway 1 https://10.201.174.36/SSLVPNphone
 vpn-trustpoint 1 trustpoint cme_cert root
 vpn-hash-algorithm sha-1
vpn-profile 1
 host-id-check disable
 sip
!
!
!
ip http server
no ip http secure-server
!
telephony-service
 max-ephones 20
 max-dn 10
 ip source-address 10.201.160.201 port 2000
 cnf-file location flash:
 cnf-file perphone
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-dn 1
 number 2223
 label TestPhone
!
!
ephone 1
 device-security-mode none
 mac-address 001F.6C81.110E
 type 7965
 vpn-group 1
 vpn-profile 1
 button 1:1
!
end
```

Example for Configuring SSL VPN with DTLS on CME as VPN Headend

The following example shows how to configure CME using DTLS on CME as VPN Headend:

```
!
ip domain-name cisco.com
!
aaa new-model
!
!
aaa authentication login default local
!
!
!
crypto pki server cme_root
 database level complete
 no database archive
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
!
crypto pki trustpoint cme_root
 enrollment url http://10.201.160.201:80
 revocation-check none
 rsakeypair cme_root
!
crypto pki trustpoint cme_cert
 enrollment url http://10.201.160.201:80
 revocation-check none
!
```

```
crypto pki trustpoint TP-self-signed-4067918560
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4067918560
 revocation-check none
 rsakeypair TP-self-signed-4067918560
!
!
!
voice service voip
vpn-group 1
 vpn-gateway 1 https://10.201.160.201/SSLVPNphone
 vpn-trustpoint 1 trustpoint cme_cert leaf
 vpn-hash-algorithm sha-1
vpn-profile 1
 host-id-check disable
sip
!
username kurt privilege 15 password 0 cisco
!
!
interface GigabitEthernet0/0
 ip address 10.201.160.201 255.255.255.192
 duplex auto
 speed auto
!
ip local pool SSLVPNphone_pool 10.201.160.202 10.201.160.203
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
!
telephony-service
 max-ephones 20
 max-dn 10
 ip source-address 10.201.160.201 port 2000
 cnf-file location flash:
 cnf-file perphone
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-dn 1
 number 2223
 label TestPhone
!
!
ephone 1
 device-security-mode none
 mac-address 001F.6C81.110E
 type 7965
 vpn-group 1
 vpn-profile 1
 button 1:1
!
webvpn gateway sslvpn_gw
 ip address 10.201.160.201 port 443
 ssl encryption 3des-sha1 aes128-sha1
 ssl trustpoint cme_cert
 inservice
!
webvpn context SSLVPNphone
gateway sslvpn_gw domain SSLVPNphone
ca trustpoint cme_cert
!
ssl authenticate verify all
inservice
!
policy group SSLVPNphone
 functions svc-enabled
 svc address-pool "SSLVPNphone_pool" netmask 255.255.255.224
 svc default-domain "cisco.com"
```

```
 hide-url-bar
 default-group-policy SSLVPNphone
!
end
```

The following example shows the vpn configuration:

```
Router #show voice vpn
The Voice Service VPN Group 1 setting:
VPN Gateway 1 URL https://9.10.60.254/SSLVPNphone
VPN Trustpoint hash in sha-1
VPN Trustpoint 1 trustpoint cme_cert root fbUqFIbtWtaYSGSlTP/Umshcgyk= The Voice Service
VPN Profile 1 setting:
The host_id_check setting: 0
```

Feature Information for SSL VPN Client

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

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

Table 87: Feature Information for SSL VPN Client

Feature Name	Cisco Unified CME Versions	Feature Information
Support on Cisco Unified CME with DTLS	8.6	Introduced support on Cisco Unified CME with DTLS.
SSL VPN Client Support on SCCP IP Phones	8.5	Introduced the SSL VPN Client Support feature.

CHAPTER 38

Automatic Line Selection

This chapter describes automatic line selection feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Note This feature is applicable for SCCP phones only. For newer SIP phones (Cisco Unified IP Phone 7800, 8800 series) with new user interface, this feature is not applicable. The user selects the line and the focus would be on that selected line. Both incoming and outgoing calls changes the focus based on the line selected or line answered.

Information About Automatic Line Selection

Automatic Line Selection for Incoming and Outgoing Calls

On multiline IP phones, lifting the handset automatically selects the first ringing line on the phone or, if no line is ringing, selects the first available idle line for outgoing calls. This is the default behavior for all multiline IP phones.

Under some circumstances, however, you might want to require that a line button be explicitly pressed to select an outgoing line or to answer an incoming call. In Cisco CME 3.0 and later, you have the flexibility to assign the type of line selection that each IP phone uses.

The Automatic Line Selection feature allows you to specify, on a per-phone basis, the line that is selected when you pick up a phone handset.

Any of the following behaviors can be assigned on a per-phone basis:

- Automatic line selection—Picking up the handset answers the first ringing line or, if no line is ringing, selects the first idle line. Use the **auto-line** command with no keyword or argument. This is the default.
- Manual line selection (no automatic line selection)—Pressing the Answer soft key answers the first ringing line, and pressing a line button selects a line for an outgoing call. Picking up the handset does not answer calls or provide dial tone. Use the **no auto-line** command.
- Automatic line selection for incoming calls only—Picking up the handset answers the first ringing line, but if no line is ringing, it does not select an idle line for an outgoing call. Pressing a line button selects a line for an outgoing call. Use the **auto-line incoming** command.
- Automatic line selection for outgoing calls only—Picking up the handset for an outgoing call selects the line associated with the *button-number* argument. If a button number is specified and the line associated with that button is unavailable (because it is a shared line in use on another phone), no dial tone is heard when the handset is lifted. You must press an available line button to make an outgoing call. Incoming calls must be answered by pressing the Answer soft key or pressing a ringing line button. Use the **auto-line** command with the *button-number* argument.
- Automatic line selection for incoming and outgoing calls—Pressing the Answer soft key or picking up the handset answers an incoming call on the line associated with the specified button. Picking up the handset for outgoing calls selects the line associated with the specified button. Use the **auto-line** command with the *button-number* argument and **answer-incoming** keyword.

Configure Automatic Line Selection

Enable Automatic Line Selection

To enable automatic line selection for answering incoming calls or making outgoing calls, perform the following steps:

Restriction Automatic line selection is bypassed if it is configured for a trunk directory number and the line is seized by pressing the Park or Callfwd soft keys. The first available directory number is seized.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **auto-line** [*button-number* [**answer-incoming**] | **incoming**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 24`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number for the phone on which you want to configure automatic line selection.
Step 4	**auto-line** [*button-number* [**answer-incoming**] | **incoming**] **Example:** `Router(config-ephone)# auto-line 5 answer-incoming`	Assigns a type of line selection behavior to this phone. • **auto-line**—Picking up the handset answers the first ringing line or, if no line is ringing, selects the first idle line. This is the default. • **auto-line** *button-number*—Picking up the handset for an outgoing call selects the line associated with the specified button. The default if this argument is not used is the topmost available line. • **auto-line** *button-number***answer-incoming**—Picking up the handset answers the incoming call on the line associated with the specified button. • **auto-line incoming**—Picking up the handset answers the first ringing line but, if no line is ringing, does not select an idle line for an outgoing call. Pressing a line button selects a line for an outgoing call. • **no auto-line**—Disables automatic line selection. Pressing the Answer soft key answers the first ringing line, and pressing a line button selects a line for an outgoing call. Picking up the handset does not answer calls or provide dial tone.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verify Automatic Line Selection

Step 1 Use the **show running-config** command to verify your configuration. Automatic line selection is listed in the ephone portion of the output.

Example:

Router# **show running-config**

```
ephone  2
headset auto-answer line 1
headset auto-answer line 4
ephone-template 1
mac-address 011F.9010.1790
paging-dn 48
type 7960
no dnd feature-ring
no auto-line
```

Step 2 Use the **show telephony-service ephone** command to display only ephone configuration information.

Example:

Router# **show telephony-service ephone**

```
ephone 4
 device-security-mode none
 username "Accounting"
 mac-address FF0E.4857.5E91
 button 1c34,35
 no auto-line
```

Configuration Examples for Automatic Line Selection

Example for Automatic Line Selection

The following example assigns no automatic line selection to phones 1 and 2 and assigns automatic line selection for incoming calls only to phone 3:

```
ephone 1
mac-address 00e0.8646.9242
button 1:1 2:4 3:16
no auto-line
!
ephone 2
mac-address 01c0.4612.7142
button 1:5 2:4 3:16
no auto-line
!
ephone 3
mac-address 10b8.8945.3251
button 1:6 2:4 3:16
auto-line incoming
```

The following example enables automatic selection of line button 1 when the handset is lifted to answer incoming calls or to make outgoing calls.

```
ephone  1
mac-address 0001.0002.0003
type 7960
```

```
auto-line 1 answer-incoming
button  1:1 2:2 3:3
```

Feature Information for Automatic Line Selection

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

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

Table 88: Feature Information for Automatic Line Selection

Feature Name	Cisco Unified CME Version	Feature Information
Automatic Line Selection	4.0	The **answer-incoming** keyword was added to the **auto-line** command.
	3.1	The *button-number* argument was added to the **auto-line** command.
	3.0	Automatic line selection was introduced.

CHAPTER 39

Barge and Privacy

Information About Barge and Privacy

Barge and cBarge

The Barge feature enables phone users who share a directory number to join an active call on the shared line by pressing a softkey. When the initiator barges into a call, a conference is created between the barge initiator, the target party, and the other party connected in the call. Parties see the call information on their phones and, if the conference join tone is configured, hear a tone.

If a phone that is using the shared line has Privacy enabled, call information does not appear on the other phones that share the line and the call cannot be barged. Connected parties hear the barge tone (single beep) after the conference is set up. When a party leaves the conference, a barge leave tone is played to the remaining parties.

From Cisco Unified CME Release 11.7 onwards, cBarge feature is supported on Cisco 4000 Series Integrated Services Router.

From Cisco Unified CME Release 12.0 onwards, cBarge feature is supported with mixed shared line.

Note

- Cisco Unified IP Phone 69xx series do not support cBarge with Unified CME.
- Barge and Cbarge softkeys on SIP Phones are supported only on shared lines.

Barge (SIP)

Barge uses the built-in conference bridge on the target phone (the phone that is being barged) which limits the number of users allowed to barge. A barge conference supports up to three parties. If more users want to join a call on a SIP shared line, cBarge must be used. The SIP phone requires the built-in conference bridge to use Barge. Barge is supported for SIP shared-line directory numbers only.

Note If a phone user barges into a barge conference, the conference is converted to a cBarge conference.

cBarge (SCCP and SIP)

The cBarge feature uses a shared conference resource which allows more that one person to barge into the call. A cBarge conference supports the maximum number of parties provisioned on the centralized conference resource. The centralized conference resource must be provisioned to use cBarge. cBarge is supported on SCCP shared octo-line directory numbers and SIP shared-line directory numbers.

When any party releases from the call, the call remains a conference call if at least three participants remain on the line. If only two parties remain in the conference, they are reconnected as a point-to-point call, which releases the conference bridge resources. When the target party parks the call or joins the call with another call, the barge initiator and the other parties remain connected.

Table 89: Barge and cBarge Call Differences between Built-In and Shared Conference Bridge, on page 1048 describes the differences between Barge using a built-in conference bridge and cBarge using a shared conference bridge.

Table 89: Barge and cBarge Call Differences between Built-In and Shared Conference Bridge

Action	Barge—Built-In Conference Bridge at Target Device	cBarge—Shared Conference Bridge
Media break occurs during barge setup	No	Yes
User receives a Barge tone, if configured	Yes	Yes
Displays name at barge initiator phone	To Barge	To Barge
Displays name at target phone	To/From Other	To Barge
Displays name at other phones	To/From Target	To Barge
Allows second barge setup to an already barged call	Yes	Yes
Maximum number of parties	3	Maximum allowed by the shared conference resource.

Action	Barge—Built-In Conference Bridge at Target Device	cBarge—Shared Conference Bridge
Initiator releases call	No media interruption occurs for the two original parties.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Target releases call	Media break occurs to reconnect initiator with the other party as a point-to-point call.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Other party releases call	All three parties are released.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Target puts call on hold and performs Transfer, Conference, or Call Park.	Initiator is released.	Initiator and the other party remain connected.

If no conference bridge is available, either built-in at the target device for barge or shared for cBarge, or the maximum number of participants is reached, Cisco Unified CME rejects the barge request and an error message displays on the initiating phone.

The barge and cBarge soft keys display by default when a phone user presses the shared-line button for an active remote-in-use call. The user selects either barge or cBarge to join the shared-line call. When there are multiple active calls on the shared line, the barge initiator can select which call to join by highlighting the call.

You can customize the soft key display with a soft key template. For configuration information, see Configure the cBarge Soft Key on SCCP Phones, on page 1050 or Enable Barge and cBarge Soft Keys on SIP Phones, on page 1052.

Restriction cBarge operation on an existing ad-hoc or meet-me conference is not supported.

Privacy and Privacy on Hold

The privacy feature enables phone users to block other users who share a directory number from seeing call information, resuming a call, or barging into a call on the shared line. When a phone receives an incoming call on a shared line, the user can make the call private by pressing the Privacy feature button, which toggles between on and off to allow the user to alter the privacy setting on their phone. The privacy state is applied to all new calls and current calls owned by the phone user.

Privacy is supported on SCCP octo-line directory numbers and SIP shared-line directory numbers.

Privacy is enabled for all phones in the system by default. You can disable privacy globally and enable it only for specific phones, either individually or through an phone template. You can also enable the privacy button on specific phones. After a phone with the privacy button enabled registers with Cisco Unified CME, the line feature button on the phone gets labeled "Privacy," a status icon displays, and if the button has a monitor lamp, it lights when privacy is active. For Extension Mobility phones, you can enable the privacy button in the user profile and logout profile.

The Privacy on Hold feature prevents other phone users from viewing call information or retrieving a call put on hold by another phone sharing the directory number. Privacy on Hold is disabled for all phones in the system by default. You can enable Privacy on Hold globally for all phones. To disable Privacy on Hold on individual phones, you must disable Privacy on those phones.

The Privacy feature applies to all shared lines on a phone. If a phone has multiple shared lines and Privacy is enabled, other phones cannot view or barge into calls on any of the shared lines.

For SCCP configuration information, see Enable Privacy and Privacy on Hold on SCCP Phones, on page 1054.

For SIP configuration information, see Enable Privacy and Privacy on Hold on SIP Phones, on page 1057.

Configure Barge and Privacy

Configure the cBarge Soft Key on SCCP Phones

To enable a phone user to join a call on an octo-line directory number by pressing the cBarge soft key, perform the following steps. The cBarge soft key is enabled by default. This task is required only if you want to change the order of the soft key display during the remote-in-use call state.

Restriction

- Supported only on octo-line directory numbers.
- Not supported for meet-me conferences.
- Not supported if phone user is already connected to the same ad hoc conference on the octo-line.

Before You Begin

- Cisco Unified CME 7.0 or a later version.
- Octo-line directory number is configured. See Create Directory Numbers for SCCP Phones, on page 253.
- Privacy is disabled on the phone. See Privacy and Privacy on Hold, on page 1049.
- Ad hoc hardware conference resource is configured and ready to use. See Configure Conferencing, on page 1377.
- Join and leave tones for hardware conference can be configured as barge entrance and exit tones. See Configure Join and Leave Tones on SCCP Phones, on page 1384.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **softkeys remote-in-use** {[**CBarge**] [**Newcall**]}
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone-template** *template-tag* **Example:** `Router(config)# ephone-template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 20.
Step 4	**softkeys remote-in-use** {[**CBarge**] [**Newcall**]} **Example:** `Router(config-ephone-template)# softkeys remote-in-use CBarge Newcall`	Modifies the order and type of soft keys that display on an IP phone during the remote-in-use call state.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag*	Applies the ephone template to the phone.

	Command or Action	Purpose
	Example: `Router(config-ephone)# ephone-template 5`	• *template-tag*—Unique identifier of the ephone template that you created in Step 3.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Examples

The following example shows that ephone template 5 modifies the soft keys displayed for the remote-in-use call state and it is applied to ephone 12:

```
ephone-template  5
 softkeys remote-in-use  CBarge Newcall
 softkeys hold  Resume Newcall Join
 softkeys connected  TrnsfVM Park Acct ConfList Confrn Endcall Trnsfer Hold
 max-calls-per-button 3
 busy-trigger-per-button 2
!
!
ephone  12
 no phone-ui speeddial-fastdial
 ephone-template 5
 mac-address 000F.9054.31BD
 type 7960
 button  1:10 2:7
```

Enable Barge and cBarge Soft Keys on SIP Phones

A phone user can join a call on a shared line by pressing the Barge or cBarge soft keys. The Barge and cBarge soft keys are enabled by default on supported SIP phones. Perform the following steps only if you want to change the order or appearance of soft keys displayed during the remote-in-use call state.

Restriction

• Supported only on shared lines.

Before You Begin

• Cisco Unified CME 7.1 or a later version.

• Shared directory number is configured. See Create Directory Numbers for SIP Phones, on page 263.

• Ad hoc hardware conference resource is configured and ready to use. See Configure Conferencing, on page 1377.

• Join and leave tones for hardware conference can be configured as barge entrance and exit tones. See Configure Join and Leave Tones on SCCP Phones, on page 1384 in the *Cisco Unified CME System Administrator Guide*.

- For Barge and cBarge to work, privacy needs to be disabled under voice register global using the command **no privacy**. For configuring Privacy, See Enable Privacy and Privacy on Hold on SIP Phones, on page 1057.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **softkeys remote-in-use** {[**Barge**] [**Newcall**] [**cBarge**]}
5. **exit**
6. **voice register pool** *phone-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters voice register template configuration mode to create a voice register template. • *template-tag*—Unique identifier for the voice register template that is being created. Range: 1 to 10.
Step 4	**softkeys remote-in-use** {[**Barge**] [**Newcall**] [**cBarge**]} **Example:** `Router(config-register-temp)# softkeys remote-in-use cBarge Newcall`	Modifies the order and type of soft keys that display on a SIP phone during the remote-in-use call state.
Step 5	**exit** **Example:** `Router(config-register-temp)# exit`	Exits voice register template configuration mode.
Step 6	**voice register pool** *phone-tag*	Enters voice register pool configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# voice register pool 12`	• *phone-tag*—Unique number that identifies this voice register pool during configuration tasks.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the voice register template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows that voice register template 5 modifies the soft keys displayed for the remote-in-use call state and it is applied to phone 120:

```
voice register template  5
 softkeys hold  Resume Newcall
 softkeys connected  Trnsfer Park Hold
 softkeys remote-in-use  cBarge Barge
!
voice register pool  120
 id mac 0030.94C2.A22A
 type 7962
 number 1 dn 20
 template 5
```

Enable Privacy and Privacy on Hold on SCCP Phones

To enable Privacy and Privacy on Hold on SCCP phones, perform the following steps.

- If all phones require access to privacy, leave the system-level **privacy** (telephony-service) command set to enabled (default value) and leave the phone-level **privacy** (ephone) command set to the default (use system value).
- If only specific phones require access to privacy, disable privacy at the system-level by using the **no privacy** command in telephony-service configuration mode and enable privacy at the phone-level by using the **privacy on** command in ephone or ephone-template configuration mode.
- Enable Privacy on Hold at the system-level. To disable Privacy on Hold on individual phones, you must disable Privacy on those phones.

Restriction

- Privacy and Privacy on Hold are supported for calls on shared octo-line directory numbers only.
- Privacy and Privacy on Hold are not supported on the Cisco Unified IP Phone 7935, 7936, 7937, or 7985, Nokia E61, analog phones connected to the Cisco VG224 or Cisco ATA, or any phone without a display.

Before You Begin

- Cisco Unified CME 7.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **privacy**
5. **privacy-on-hold**
6. **exit**
7. **ephone** *phone-tag*
8. **privacy** [**off** | **on**]
9. **privacy-button**
10. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**privacy** **Example:** `Router(config-telephony)# privacy`	(Optional) Enables privacy at the system-level for all phones. • This command is enabled by default.

	Command or Action	Purpose
		• To enable privacy for individual phones only, disable privacy at the system-level with the **no privacy** command and enable it for individual phones as shown in Step 8.
Step 5	**privacy-on-hold** **Example:** `Router(config-telephony)# privacy-on-hold`	(Optional) Enables privacy on hold at the system-level for all phones. • Blocks phone users on shared lines from viewing call information or retrieving calls on hold. Default is disabled.
Step 6	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 7	**ephone** *phone-tag* **Example:** `Router(config)# ephone 10`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 8	**privacy** [**off** | **on**] **Example:** `Router(config-ephone)# privacy on`	(Optional) Modifies privacy support on the specific phone. • **off**—Disables privacy on the phone. • **on**—Enables privacy on the phone. • System-level privacy setting is the default. Use this command only if you want to modify the system-level setting in Step 4 for a specific phone. • Using the **no** form of this command to reset to the system-level value. • This command can also be configured in ephone-template configuration mode and applied to one or more phones. The ephone configuration has priority over the ephone-template configuration.
Step 9	**privacy-button** **Example:** `Router(config-ephone)# privacy-button`	Enables the privacy feature button on the IP phone. • Enable this command only on phones that share an octo-line directory number. • This command can also be configured in ephone-template configuration mode and applied to one or more phones. The ephone configuration has priority over the ephone-template configuration.
Step 10	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

The following example shows privacy disabled at the system-level and enabled on an individual phone. It also shows Privacy on Hold enabled at the system-level.

```
telephony-service
 no privacy
 privacy-on-hold
 max-ephones 100
 max-dn 240
 timeouts transfer-recall 60
 voicemail 8900
 max-conferences 8 gain -6
 transfer-system full-consult
 fac standard
!
!
ephone  10
 privacy on
 privacy-button
 max-calls-per-button 3
 busy-trigger-per-button 2
 mac-address 00E1.CB13.0395
 type 7960
 button  1:7 2:10
```

Enable Privacy and Privacy on Hold on SIP Phones

To enable Privacy and Privacy on Hold on SIP phones, perform the following steps.

- To enable Privacy on all phones, leave the system-level **privacy** (voice register global) command set to enabled (default value) and leave the phone-level **privacy** (voice register pool) command set to the default (use system value).
- To enable Privacy on specific phones only, disable privacy at the system-level by using the **no privacy** command in voice register global configuration mode and enable privacy at the phone-level by using the **privacy on** command in voice register pool or voice register template configuration mode.
- To enable Privacy on Hold on all phones, enable it at the system-level with the **privacy-on-hold** command. To disable Privacy on Hold on specific phones, disable Privacy on those phones using the **privacy off** command in voice register pool or voice register template configuration mode. Privacy must be enabled to support Privacy on Hold.

Restriction

- Privacy and Privacy on Hold are supported for calls on shared-line directory numbers only.
- Privacy and Privacy on Hold are not supported on the Cisco Unified IP Phone 7935, 7936, 7937, or 7985, Nokia E6, analog phones connected to the Cisco VG224 or Cisco ATA, or any phone without a display.

Before You Begin

- Cisco Unified CME 7.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **privacy**
5. **privacy-on-hold**
6. **exit**
7. **voice register pool** *phone-tag*
8. **privacy** {**off** | **on**}
9. **privacy-button**
10. **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 register global** **Example:** `Router(config)# voice register global`	Enters telephony-service configuration mode.
Step 4	**privacy** **Example:** `Router(config-register-global)# privacy`	(Optional) Enables privacy at the system-level for all phones. • This command is enabled by default. • To enable privacy for individual phones only, disable privacy at the system-level with the **no privacy** command and enable it for individual phones as shown in Step 8.
Step 5	**privacy-on-hold** **Example:** `Router(config-register-global)# privacy-on-hold`	(Optional) Enables privacy on hold at the system-level for all phones. • Blocks phone users on shared lines from viewing call information or retrieving calls on hold. Default is disabled.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global configuration mode.
Step 7	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 10`	Enters voice register pool configuration mode. • *phone-tag*—Unique number that identifies this phone during configuration tasks.
Step 8	**privacy** {**off** | **on**} **Example:** `Router(config-register-pool)# privacy on`	(Optional) Modifies phone-level privacy setting on this phone. The default value is the system setting. • **off**—Sets privacy state to off on the phone. • **on**—Sets privacy state to on for the phone • Use this command only if you want to modify the system-level setting in Step 4 for a specific phone. • Using the **no** form of this command to reset to the system-level value. • This command can also be configured in voice register template configuration mode and applied to one or more phones. The phone configuration has priority over the phone template configuration.
Step 9	**privacy-button** **Example:** `Router(config-register-pool)# privacy-button`	Enables the privacy feature button on the IP phone. • Enable this command only on phones with a shared-line directory number. • This command can also be configured in voice register template configuration mode and applied to one or more phones. The phone configuration has priority over the phone template configuration.
Step 10	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows privacy disabled at the system-level and enabled on an individual phone. It also shows Privacy on Hold enabled at the system-level.

```
voice register global
```

```
 mode cme
 privacy-on-hold
 no privacy
 max-dn 300
 max-pool 150
 voicemail 8900
!
!
voice register pool  130
 id mac 001A.A11B.500E
 type 7941
 number 1 dn 30
 privacy ON
 privacy-button
```

Feature Information for Barge and Privacy

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

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

Table 90: Feature Information for Barge and Privacy

Feature Name	Cisco Unified CME Version	Modification
Barge	12.0	Added cBarge support for mixed shared line.
	11.7	Added support for cBarge on Cisco 4000 Series Integrated Services Router for Unified CME.
	7.1	Added Barge and cBarge support for SIP shared-line directory numbers.
	7.0/4.3	Added cBarge support for SCCP shared octo-line directory numbers.
Privacy	7.1	Added support for Privacy on SIP shared-line directory numbers.
	7.0/4.3	Added support for Privacy on SCCP shared octo-line directory numbers.

CHAPTER 40

Call Blocking

Information About Call Blocking

Call Blocking Based on Date and Time (After-Hours Toll Bar)

Call blocking to prevent unauthorized use of phones is implemented by matching dialed numbers against a pattern of specified digits and matching the time against the time of day and day of week or date that has been specified for Call Blocking. You can specify up to 32 patterns of digits for blocking.

When a user attempts to place a call to digits that match a pattern that has been specified for Call Blocking during a time period that has been defined for Call Blocking, 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.

The Cisco Unified CME session application accesses the current after-hours configuration and applies it to calls originated by phones that are registered to the Cisco Unified CME router. Call blocking applies to all IP phones in Cisco Unified CME, although individual IP phones can be exempted from all call blocking.

In Cisco CME 3.4 and later versions, the same time-based call-blocking mechanism that is provided for SCCP phone and on analog phones connected to SCCP-controlled analog telephone adaptors (Cisco ATA) or SCCP-controlled foreign exchange station (FXS) ports is expanded to SIP endpoints.

In Cisco CME 3.4 and later, call-blocking configuration applies to all SCCP, H.323, SIP and POTS calls that go through the Cisco Unified CME router. All incoming calls to the router, except calls from an exempt phone, are also checked against the after-hours configuration.

Prior to Cisco Unified CME 4.2(1), all Call Blocking features are implemented globally and uniformly on each phone in the system. All phones are similarly restricted according to time, date, location, and other call blocking characteristics. Call Blocking is not supported on ephone-dns that are configured to use the trunk feature, and Call Blocking did not apply to second-stage trunk dialing.

In Cisco Unified CME 4.2(1) and later versions, you have the flexibility to set different call block calendars and call block patterns to phones in different departments, to block certain trunk dialing as required, and to configure Call Blocking on a particular SCCP IP phone by creating and applying a template to that phone.

For configuration information, see Configure Call Blocking, on page 1064.

After-Hours Pattern-Blocking Support for Regular Expressions

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

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

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

after-hours block pattern *pattern-tag pattern*

This command is available in the following configuration modes:

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

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

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

- numbers beginning with ‘0’ and ‘00’
- numbers beginning with 1800, followed by four digits
- numbers 9876512340 to 9876512345

then the following configurations can be used:

- after-hours block pattern 1 0*
- after-hours block pattern 2 00*
- after-hours block pattern 3 1800….
- after-hours block pattern 4 987651234[0-5]

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

After-hours block pattern 0* blocks all numbers, and 00* blocks any number starting from 0. 0* and 00* must not be denoted as regular expressions.

For more configuration examples, see Example for Configuring After-Hours Block Patterns of Regular Expressions, on page 1078 section.

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

Call Blocking Override

The after-hours configuration applies globally to all dial peers in Cisco Unified CME. You can disable the feature on phones using one of three mechanisms:

- directory number—To configure an exception for an individual directory number.
- phone-level—To configure an exception for all directory numbers associated to a Cisco Unified IP phone regardless of any configuration for an individual directory number.
- dial peer—To configure an exception for a particular dial peer.

Individual phone users can be allowed to override call blocking associated with designated time periods by entering personal identification numbers (PINs) that have been assigned to their phones. For IP phones that support soft keys, such as the Cisco Unified IP Phone 7940G and the Cisco Unified IP Phone 7960G, the call-blocking override feature allows individual phone users to override the call blocking that has been defined for designated time periods. The system administrator must first assign a personal identification number (PIN) to any phone that will be allowed to override Call Blocking.

Logging in to a phone with a PIN only allows the user to override call blocking that is associated with particular time periods. Blocking patterns that are in effect 7 days a week, 24 hours a day, and they cannot be overridden by using a PIN.

When PINs are configured for call-blocking override, they are cleared at a specific time of day or after phones have been idle for a specific amount of time. The time of day and amount of time can be set by the system administrator, or the defaults can be accepted.

For configuration information, see Configure Call Blocking, on page 1064.

Class of Restriction

Class of restriction (COR) is the capability to deny certain call attempts based on the incoming and outgoing class of restrictions provisioned on the dial peers. COR specifies which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list.

COR functionality provides flexibility in network design by allowing users to block calls (for example, calls to 900 numbers) and allowing different restrictions to call attempts from different originators.

For SIP phones, multiple COR lists can be applied under the voice register pool. A maximum of ten lists (five incoming and five outgoing) can be defined. The final COR list that is applied depends on the DN that the phone registers with the CME. This DN should match any one of the ranges defined in the COR list under the voice register pool.

For SIP Phones on Unified CME Release 12.1 and later versions, COR lists can be applied under voice register template configuration mode as well. If the COR list is configured under voice register pool and voice register template, the configuration under voice register pool takes precedence. If the COR list configuration under voice register pool is removed, the configuration under voice register template is applied.

Configure Call Blocking

Configure Call Blocking

To define blocking patterns and time periods during which calls to matching patterns are blocked for all SCCP and SIP endpoints in Cisco Unified CME, to define blocking patterns to be matched to block calls from PSTN lines, and to deactivate logins on SCCP phones at a specific time or for a specified time period, perform the following steps.

Restriction

- Prior to Cisco CME 3.3, Call Blocking is not supported on analog phones connected to Cisco ATAs or FXS ports in H.323 mode.
- Prior to Cisco CME 3.4, Call Blocking is not supported on SIP IP phones connected directly in Cisco Unified CME.
- Prior to Cisco Unified CME 4.2(1), selective Call Blocking on IP phones and PSTN trunk lines is not supported.

Before You Begin

- Dial-peers are configured to provide PSTN access using router voice-ports or H.323/SIP trunk connections.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony service**
4. **after-hours block pattern** *pattern-tag pattern* [**7-24**]
5. **after-hours date** *month date start-time stop-time*
6. **after-hours day** *day start-time stop-time*
7. **after-hours pstn-prefix** *tag pattern*
8. **login** [**timeout** [*minutes*]] [**clear** *time*]
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony service** **Example:** `Router(config)# telephony service`	Enters telephony service configuration mode.
Step 4	**after-hours block pattern** *pattern-tag pattern* [**7-24**] **Example:** `Router(config-telephony)# after-hours block pattern 2 91`	Defines pattern to be matched for blocking calls from IP phones. • *pattern-tag*—Unique number pattern for call blocking. Define up to 32 call-blocking patterns in separate commands. Range is 1 to 32. • This command can also be configured in ephone-template configuration mode. The value set in ephone-template configuration mode has priority over the value set in telephony-service mode .
Step 5	**after-hours date** *month date start-time stop-time* **Example:** `Router(config-telephony)# after-hours date jan 1 0:00 23:59`	Defines a recurring period based on date of month during which outgoing calls that match defined block patterns are blocked on IP phones. • Enter beginning and ending times for call blocking in an HH:MM format using a 24-hour clock. The *stop- time* must be greater than the *start-time*. The value 24:00 is not valid. If you enter 00:00as a stop time, it is changed to 23:59. If you enter 00:00 for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date. • This command can also be configured in ephone-template configuration mode. The value set in ephone-template configuration mode has priority over the value set in telephony-service mode.
Step 6	**after-hours day** *day start-time stop-time* **Example:** `Router(config-telephony)# after-hours day sun 0:00 23:59`	Defines a recurring period based on day of the week during which outgoing calls that match defined block patterns are blocked on IP phones • Enter beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. The *stop- time* must be greater than the *start-time*. The value 24:00 is not valid. If you enter 00:00 as a stop time, it is changed to 23:59. If you enter 00:00 for both start time and stop time, calls are blocked for the entire 24-hour period on the specified day. • This command can also be configured in ephone-template configuration mode. The value set in ephone-template configuration mode has priority over the value set in telephony-service mode .
Step 7	**after-hours pstn-prefix** *tag pattern* **Example:** `Router(config-telephony)# after-hours pstn_prefix 1 9`	Defines the leading digits of the pattern to be skipped when pattern matching dialed digits on a trunk ephone-dn. • *tag*: Unique number pattern for PSTN call blocking. Define up to 4 call-blocking patterns in separate commands. Range is 1-4.

	Command or Action	Purpose
		• *pattern*: identifies the unique leading digits, normally used to dial a trunk PSTN line, that are blocked by this configuration.
Step 8	**login** [**timeout** [*minutes*]] [**clear** *time*] **Example:** `Router(config-telephony)# login timeout 120 clear 23:00`	Deactivates all user logins at a specific time or after a designated period of idle time on a phone. • For SCCP phones only. Not supported on SIP endpoints in Cisco Unified CME. • *minutes*—(Optional) Range: 1 to 1440. Default: 60. Before Cisco Unified CME 4.1, the minimum value for this argument was 5 minutes.
Step 9	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Call Blocking Exemption for a Dial Peer

To allow H.323 and SIP trunk calls to utilize the voice gateway in spite of the the after-hours configuration in Cisco Unified CME, follow the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag*{**pots** | **voatm** |**vofr** |**voip**}
4. **paramspace callsetup after-hours-exempt true**
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag*{**pots** | **voatm** |**vofr** |**voip**} **Example:** `Router(config)# dial peer voice 501 voip`	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial-peer configuration mode.
Step 4	**paramspace callsetup after-hours-exempt true** **Example:** `Router(config-dialpeer)#` **paramspace callsetup after-hours-exempt true**	Exempts a dial peer from Call Blocking configuration.

Step 5	**end**
	
	Example:
	`Router(config-dialpeer)# end`
	or
	`Router(config-register-dn)# end`
		Exits configuration mode and enters privileged EXEC mode.

Configure Call Blocking Override for All SCCP Phones

To define the Call Blocking override code to be entered by a phone user to override all call-blocking rules, perform the following steps.

Restriction

- Call Blocking override is supported only on phones that support softkey display.
- If the after-hours override code is the same as the night-service code, after hours Call Blocking is disabled.
- Both override codes defined in telephony-service and override codes defined in ephone-template are enabled on all phones.
- If a global telephony-service override code overlaps an ephone-template override code and contains more digits, an outgoing call is disabled wherever the telephony-service override code is used on phones with the ephone template applied. For example, if the telephony-service override code is 6241 and the ephone-template override code is 62, those phones with the ephone template applied will sound a fast busy tone if the 6241 override code is dialed.

Before You Begin

- Cisco Unified CME 4.2(1) or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **after-hours override-code** *pattern*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony service configuration mode.
Step 4	**after-hours override-code** *pattern* **Example:** `Router(config-telephony)# after-hours override-code 1234`	Defines the pattern of digits (0-9) that overrides an after-hours call blocking configuration. • *pattern*: identifies the unique set of digits that, when dialed after pressing the login soft key, can override the after-hours call blocking configuration. • This command can also be configured in ephone-template configuration mode. The value set in ephone-template configuration mode has priority over the value set in telephony-service mode.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configure Call Blocking Exemption for an Individual SCCP Phone

To exempt all directory numbers associated with an individual SCCP phone from the Call Blocking configuration, follow the steps in this section.

Restriction

- Call Blocking override is supported only on phones that support softkey display.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **after-hour exempt**
5. **pin** *pin-number*
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	**ephone** *phone-tag* **Example:** `Router(config)# ephone 4`	Enters ephone configuration mode. • *phone-tag*—The unique sequence number for the phone that is to be exempt from call blocking.
Step 4	**after-hour exempt** **Example:** `Router(config-ephone)# after-hour exempt`	Specifies that this phone is exempt from call blocking. Phones exempted in this manner are not restricted from any call-blocking patterns and no authentication of the phone user is required.
Step 5	**pin** *pin-number* **Example:** `Router(config-ephone)# pin 5555`	Declares a personal identification number (PIN) that is used to log into an ephone. • *pin-number*—Number from four to eight digits in length.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Configure Call Blocking Exemption for an Individual SIP Phone or Directory Number

To exempt all extensions associated with an individual SIP phone or an individual directory number from the Call Blocking configuration, follow the steps in this section.

Restriction

- The Login toll-bar override is not supported on SIP IP phones; there is no pin to bypass blocking on IP phones that are connected to Cisco Unified CME and running SIP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag* or **voice register dn** *dn-tag*
4. **after-hour exempt**
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 register pool** *pool-tag* or **voice register dn** *dn-tag* **Example:** `Router(config)# voice register pool 1`	Enters voice register pool configuration mode to set parameters for specified SIP phone. or

	Command or Action	Purpose
	or `Router(config)# voice register dn 1`	Enters voice register dn mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.

Step 4	**after-hour exempt**
	
	Example:
	`Router(config-register-pool)# after-hour exempt`
	or
	`Router(config-register-dn)# after-hour exempt`
		Exempts all numbers on a SIP phone from call blocking.
		or
		Exempts an individual directory number from call blocking.

Step 5	**end**
	
	Example:
	`Router(config-register-pool)# end`
	or
	`Router(config-register-dn)# end`
		Exits configuration mode and enters privileged EXEC mode.

Verify Call Blocking Configuration

Step 1 Use the **show running-config** command to display an entire configuration, including call-blocking number patterns and time periods and the phones that are marked as exempt from call blocking.

Example:

```
telephony-service
     fxo hook-flash
     load 7960-7940 P00305000600
     load 7914 S00103020002
     max-ephones 100
     max-dn 500
     ip source-address 10.115.43.121 port 2000
     timeouts ringing 10
     voicemail 7189
     max-conferences 8 gain -6
     moh music-on-hold.au
     web admin system name sys3 password sys3
     dn-webedit
     time-webedit
     transfer-system full-consult
     transfer-pattern .T
     secondary-dialtone 9
     after-hours block pattern 1 91900 7-24
     after-hours block pattern 2 9976 7-24
     after-hours block pattern 3 9011 7-24
     after-hours block pattern 4 91...976.... 7-24
    !
```

```
create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
```

Step 2 Use the **show ephone login** command to display the login status of all phones.

Example:

Router# **show ephone login**

```
ephone 1        Pin enabled:TRUE        Logged-in:FALSE
ephone 2        Pin enabled:FALSE
ephone 3        Pin enabled:FALSE
```

Step 3 The **show voice register dial-peer** command displays all the dial peers created dynamically by SIP phones that have registered, along with configurations for after hours blocking.

Apply Class of Restriction to a Directory Number on SCCP Phone

To apply a class of restriction to a directory number, perform the following steps.

Restriction

- In a Call Redirection scenario (either Call Forward or Call Forward Busy), when you select an outgoing dial peer, CUCME considers the Class of Restriction applied on the originating extension instead of the one applied on the redirecting extension. This is because the redirecting extension is an intermediate dial peer that is used temporarily.

Before You Begin

- COR lists must be created in dial peers. For information, see Class of Restrictions section in the "*Dial Peer Configuration on Voice Gateway Routers*" document in the Cisco IOS Voice Configuration Library.
- Directory number to which COR is to be applied must be configured in Cisco Unified CME. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **corlist** {**incoming** | **outgoing**} *cor-list-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 12`	Enters ephone-dn configuration mode.
Step 4	**corlist** {**incoming** | **outgoing**} *cor-list-name* **Example:** `Router(config-ephone-dn)# corlist outgoing localcor`	Configures a COR on the dial peers associated with an ephone-dn.
Step 5	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Apply Class of Restriction to Directory Number on SIP Phones

To apply a class of restriction to virtual dial peers for directory numbers associated with a SIP IP phone connected to Cisco Unified CME, perform the following steps.

Restriction

- In a Call Redirection scenario (either Call Forward or Call Forward Busy), when you select an outgoing dial peer, CUCME considers the Class of Restriction applied on the originating extension instead of the one applied on the redirecting extension. This is because the redirecting extension is an intermediate dial peer that is used temporarily.

Before You Begin

- Cisco unified CME 3.4 or a later version.
- COR lists must be created in dial peers. For information, see Class of Restrictions section in the "*Dial Peer Configuration on Voice Gateway Routers*" document in the *Cisco IOS Voice Configuration Library*.
- Individual phones to which COR is to be applied must be configured in Cisco Unified CME. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

- The COR list configuration under voice register template configuration mode is supported only for Unified CME 12.1 and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
    - **voice register pool** *pool-tag*
    - **voice register template** *template-tag*
4. **cor**{**incoming** | **outgoing**} *cor-list-name* {*cor-list-number starting-number* [**-** *ending-number*] | **default**}
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	Enter one of the following commands: • **voice register pool** *pool-tag* • **voice register template** *template-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone in Cisco Unified CME. • *pool-tag*—Unique number assigned to the pool. Range is 1 to 100. or Enters voice register template configuration mode and defines a template of common parameters for Cisco Unified SIP IP phones. • *template-tag*—Declares a template tag. Range is 1 to 10.
Step 4	**cor**{**incoming** | **outgoing**} *cor-list-name* {*cor-list-number starting-number* [**-** *ending-number*] | **default**} **Example:** `Router(config-register-pool)# cor incoming call91191011`	Configures a class of restriction (COR) for the dynamically created VoIP dial peers associated with directory numbers and specifies which incoming dial peer can use which outgoing dial peer to make a call. • Each dial peer can be provisioned with an incoming and an outgoing COR list.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Verify Class of Restriction

Step 1 Use the **show running-config** command or the **show telephony-service ephone-dn** command to verify whether the COR lists have been applied to the appropriate ephone-dns.

Example:

```
Router# show running-config

ephone-dn 23
 number 2835
 corlist outgoing 5x
```

Step 2 Use the **show dialplan dialpeer** command to determine which outbound dial peer is matched for an incoming call, based on the COR criteria and the dialed number specified in the command line. Use the **timeout** keyword to enable matching variable-length destination patters associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.

Example:

```
Router# show dialplan dialpeer 300 number 1900111

VoiceOverIpPeer900
        information type = voice,
        description = `',
        tag = 900, destination-pattern = `1900',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 900, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem passthrough = system,
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:to900
        type = voip, session-target = `ipv4:1.8.50.7',
        technology prefix:
        settle-call = disabled
        ...
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
```

```
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 19001111   Digits: 4
Target: ipv4:1.8.50.7
```

Step 3 Use the **show dial-peer voice** command to display the attributes associated with a particular dial peer.

Example:

```
Router# show dial-peer voice 100

VoiceEncapPeer100
        information type = voice,
        description = `',
        tag = 100, destination-pattern = `',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 100, Admin state is up, Operation state is up,
        Outbound state is up,
        incoming called-number = `555....', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: 'vxml_inb_app'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `',
        forward-digits default
        session-target = `', voice-port = `',
        direct-inward-dial = disabled,
        digit_strip = enabled,
        register E.164 number with GK = TRUE

        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
```

Configuration Examples for Call Blocking

Example for Configuring Call Blocking

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. The IP phone with tag number 23 and MAC address 00e0.8646.9242 is not restricted from calling any of the blocked patterns.

```
telephony-service
 after-hours block pattern 1 91
 after-hours block pattern 2 9011
 after-hours block pattern 3 91900 7-24
```

```
 after-hours day mon 19:00 07:00
 after-hours day tue 19:00 07:00
 after-hours day wed 19:00 07:00
 after-hours day thu 19:00 07:00
 after-hours day fri 19:00 07:00
 after-hours day sat 13:00 12:00
 after-hours day sun 12:00 07:00
!
ephone 23
 mac 00e0.8646.9242
 button 1:33
 after-hour exempt
!
ephone 24
 mac 2234.1543.6352
 button 1:34

The following example deactivates a phone's login after three hours of idle time and clears
 all logins at 10 p.m.:
ephone 1
 pin 1000
!
telephony-service
 login timeout 180 clear 2200
```

Example for Configuring Class of Restriction

The following example shows three dial peers for dialing local destinations, long distance, and 911. COR list user1 can access the dial peers used to call 911 and local destinations. COR list user2 can access all three dial peers. Ephone-dn 1 is assigned COR list user1 to call local destinations and 911, and ephone-dn 2 is assigned COR list user2 to call 911, local destinations, and long distance.

```
dial-peer cor custom
 name local
 name longdistance
 name 911
!
dial-peer cor list call-local
 member local
!
dial-peer cor list call-longdistance
 member longdistance
!
dial-peer cor list call-911
 member 911
!
dial-peer cor list user1
 member 911
 member local
!
dial-peer cor list user2
 member 911
 member local
 member longdistance
!
dial-peer voice 1 pots
 corlist outgoing call-longdistance
 destination-pattern 91..........
 port 2/0/0
 prefix 1
!
dial-peer voice 2 pots
 corlist outgoing call-local
 destination-pattern 9[2-9]......
 port 2/0/0
 forward-digits 7
!
dial-peer voice 3 pots
```

```
 corlist outgoing call-911
 destination-pattern 9911
 port 2/0/0
 prefix 911
!
ephone-dn 1
 corlist incoming user1
 corlist outgoing user1
!
ephone-dn 2
 corlist incoming user2
 corlist outgoing user2
```

Example for Configuring After-Hours Block Patterns of Regular Expressions

The following example shows how to configure several afterhours block patterns of regular expressions:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# telephony-service

Router(config-telephony)# after-hours block pattern 1 ?
  WORD  Specific block pattern or a regular expression for after-hour block
        pattern

Router(config-telephony)# after-hours block pattern 1 1234
Router(config-telephony)# after-hours block pattern 2 .T
Router(config-telephony)# after-hours block pattern 3 987654([1-3])+
Router(config-telephony)# after-hours block pattern 4 98765432[1-9]
Router(config-telephony)# after-hours block pattern 5 98765(432|422|456)
```

Where to Go Next

After modifying a configuration for a Cisco Unified IP phone connected to Cisco Unified CME, you must reboot the phone to make the changes take effect. For more information, see Reset and Restart Cisco Unified IP Phones, on page 397 .

Soft Key Control

To move or remove the Login soft key on one or more phones, create and apply an ephone template that contains the appropriate **softkeys** commands.

For more information, see Customize Softkeys, on page 925.

Ephone-dn Templates

The **corlist** command can be included in an ephone-dn template that is applied to one or more ephone-dns. For more information, see Templates, on page 1427.

Feature Information for Call Blocking

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

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

Table 91: Feature Information for Call Blocking

Feature Name	Cisco Unified CME Version	Feature Information
Call Blocking	4.2(1)	Added support for selective call blocking on IP phones and PSTN trunk lines.
	3.4	• Support for Call Blocking on SIP IP phones connected directly in Cisco Unified CME was introduced. • All incoming calls to the router, except calls from an exempt phone, are also checked against the after-hours configuration.
	3.3	Added support for Call Blocking on analog phones connected to Cisco ATAs or FXS ports in H.323 mode.
	3.0	• Call blocking based on date and time was introduced. • Override of Call Blocking was introduced.
Class of Restriction	12.1	Added support for COR configuration in voice register template configuration mode for Unified CME.
	3.4	Added support for COR on SIP IP Phones connected directly in Cisco Unified CME.
	2.0	Class of restriction was introduced.

CHAPTER 41

Call Park

Information About Call Park

Call Park Enhancements in Cisco Unified CME 7.1

Cisco Unified CME 7.1 adds Call Park support for SIP phones, introduces Park Reservation Groups, and enhances the Directed Call Park feature. Park slots can be shared among SCCP and SIP phones. For example, a call parked on a SCCP phone can be retrieved by a SIP phone on the same Cisco Unified CME router. Call Park features are available on SCCP and SIP phones that support the Park soft key. The Park soft key displays on supported phones by default.

Table describes how phone users park and retrieve calls in Cisco Unified CME 7.1 and later versions compared to previous versions. For SCCP phones, the only change is in how users perform Directed Call Park Retrieval. The Call Park method supported in previous versions of Cisco Unified CME is enabled by default. You can change the park and retrieval method only when there are no parked calls.

Feature	Cisco Unified CME 7.1 and Later Versions (SCCP and SIP Phones)[14]	Before Cisco Unified CME 7.1 (SCCP Phones Only)
Call Park (Basic)	Press Park soft key to park the call.	Press Park soft key to park the call.

Feature	Cisco Unified CME 7.1 and Later Versions (SCCP and SIP Phones)[14]	Before Cisco Unified CME 7.1 (SCCP Phones Only)
Call Park Retrieval[15]	Do one of the following: • Dial the park slot extension (SCCP and SIP). • Press Pickup soft key and dial park-slot extension (SCCP only). • Press Pickup soft key and the asterisk (*) on phone that parked the call (SCCP only).	Do one of the following: • Dial the park slot extension. • Press Pickup soft key and dial park-slot extension. • Press Pickup soft key and the asterisk (*) on phone that parked the call.
Directed Call Park	Press Transfer soft key and dial park-slot extension.	Press Transfer soft key and dial park-slot extension.
Directed Call Park Retrieval	Dial the retrieval FAC and park-slot extension.	Same as Basic Call Park Retrieval.

14 You must enable the **call-park system application** command.

15 SCCP phones support the Pickup soft key for Park Retrieval only if the **service directed-pickup** command is configured (default). Otherwise, the Pickup soft key initiates Local Group Pickup.

To enable Call Park features, see Enable Call Park or Directed Call Park, on page 1089.

Basic Call Park

The Call Park feature allows a phone user to place a call on hold at a special extension so it can be retrieved from any other phone in the system. A user parks the call at the extension, known as the **call-park** slot, by pressing the Park soft key. Cisco Unified CME chooses the next available call-park slot and displays that number on the phone. A user on another phone can then retrieve the call by dialing the extension number of the call-park slot.

You can define either a single extension number or a range of extension numbers to use as call-park slots. Each call-park slot can hold one call at a time so the number of calls that users can park is equal to the number of slots you create. If the secondary number is used to group calls together, calls are retrieved in the order in which they were parked; the call that has been parked the longest is the first call retrieved from the call-park slot.

A caller who is parked in a park slot hears the music-on-hold (MOH) audio stream if the call uses the G.711 codec or if the call uses G.729 with transcoding; otherwise, callers hear a tone on hold. Users who attempt to park a call at a busy slot hear a busy tone.

Call-park slots can also be monitored by assigning the call-park slot to a monitor button using the **button m** command. The line status shows “in use” when a call is parked in the monitored slot. A call that is parked on the monitored call-park slot can be picked up by pressing the assigned monitor button.

You can create a call-park slot that is reserved for use by one extension by assigning that slot a number whose last two digits are the same as the last two digits of the extension. When an extension starts to park a call, the system searches first for a call-park slot that has the same final two digits as the extension. If no such call-park slot exists, the system chooses an available call-park slot.

Multiple call-park slots can be created with the same extension number so that more than one call can be parked for a particular department or group of people at a known extension number. For example, at a hardware store, calls for the plumbing department can be parked at extension 101, calls for lighting can be parked at 102, and so forth. Everyone in the plumbing department knows that calls parked at 101 are for them and can pick up calls from extension 101. When multiple calls are parked at the same call-park slot number, they are picked up in the order in which they were parked; that is, the call that has been parked the longest is the first call picked up from that call-park slot number.

If multiple call-park slots use the same extension number, you must configure each ephone-dn that uses the extension number with the **no huntstop** command, except for the last ephone-dn to which calls are sent. In addition, each ephone-dn must be configured with the **preference** command. The preference numeric values must increase to match the order of the ephone-dns. That is, the lowest ephone-dn tag park-slot must have the lowest numeric preference number, and so forth. Without the configuration of the **preference** and **huntstop** commands, all calls that are parked after a second call has been parked will generate a busy signal. The caller who is being transferred to park will hear a busy signal, while the phone user who parked the call will receive no indication that the call was lost.

A reminder ring can be sent to the extension that parked the call by using the **timeout** keyword with the **park-slot** command. The **timeout** keyword and argument set the interval length during which the call-park reminder ring is timed out or inactive. If the **timeout** keyword is not used, no reminder ring is sent to the extension that parked the call. The number of timeout intervals and reminder rings are configured with the **limit** keyword and argument. For example, a limit of 3 timeout intervals sends 2 reminder rings (interval 1, ring 1, interval 2, ring 2, interval 3). The **timeout** and **limit** keywords and arguments also set the maximum time that calls stay parked. For example, a timeout interval of 10 seconds and a limit of 5 timeout intervals (**park-slot timeout 10 limit 5**) will park calls for approximately 50 seconds.

The reminder ring is sent only to the extension that parked the call unless the **notify** keyword is also used to specify an additional extension number to receive a reminder ring. When an additional extension number is specified using the **notify** keyword, the phone user at that extension can retrieve a call from this slot by pressing the PickUp soft key and the asterisk (*) key.

You can define both the length of the timeout interval for calls parked at a call-park slot and the number of timeout intervals that should occur before the call is either recalled or transferred. If you specify a transfer target in the **park-slot** command, the call is transferred to the specified target after the timeout intervals expire rather than to the primary number of the parking phone.

If a name has been specified for the call-park slot using the **name** command, that name will be displayed on a recall or transfer rather than an extension number.

You can also specify an alternate target extension at which to transfer a parked call if the recall or transfer target is in use (ringing or connected). For example, a call is parked at the private park slot for the phone with the primary extension of 2001, as shown in Figure 39: Dedicated Call Park Example, on page 1087 . After the timeouts expire, the system attempts to recall the call to extension 2001, but that line is connected to another call. The system then transfers the call to the alternate target, extension 3784.

View Active Parked Calls

You can view the list of active parked calls on SIP and SCCP phones using the phone menu by pressing the **Service** button on the phone and navigating to **My Phone Apps** > **Park List** .

To recall a call from the list of parked calls, you can select the desired call and press the **Pickup** soft key.

To refresh the list of parked calls you can press the **Update** soft key in the menu.

Latest parked call will be displayed on top of the list.

Note This feature can be configured as PLK button for SCCP and SIP Phone. For more information see Configure Feature Button on a Cisco Unified SCCP Line Key, on page 1464 and Configure Feature Button on a Cisco Unified SIP Phone Line Key, on page 1462.

Configure User Interface to View Active List of Parked Calls

This feature enables a user to view the list of active parked calls and is enabled by default.

Note You must perform this task only if the feature was previously disabled on a phone.

This feature is enabled by default for SCCP and SIP phones. For SCCP phones, this feature can be enabled and disabled. However, SIP phones do not have the enable or disable option.

Restriction

- If there are more than 20 active calls parked, then only the first 20 active parked calls will be displayed.
- Dedicated, private call-park slots configured using the reserved-for command are not supported on the phone's display.

Before You Begin

- Cisco Unified CME 10.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **phone-ui park-list**
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 4	**phone-ui park-list** **Example:** `Router(config-ephone)# phone-ui park-list`	Enables a phone user to view the list of active parked calls. • This command is enabled by default.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Directed Call Park

The Directed Call Park feature allows a phone user to transfer a call to a specific call-park slot using the Transfer soft key. For example, a customer calls a retail store and asks for the sporting goods department. The operator who answers the call transfers the call to one of the park-slots associated with the sporting goods department and pages the sporting goods department to retrieve the call. You can configure phones that support the directed call-park Busy Lamp Field (BLF) to monitor the busy and idle status of specific directed call-park slots.

In versions before Cisco Unified CME 4.0, callers can directly dial call-park slot numbers to be placed in park. If another call is already parked in the slot, the caller hears a busy tone.

In Cisco Unified CME 4.0 to Cisco Unified CME 7.0, users retrieve a call from a directed call-park slot by dialing the park-slot extension or using the PickUp soft key and dialing the park-slot extension. If no call is parked in the slot, the caller hears a busy tone.

In Cisco Unified CME 7.1 and later versions, users retrieve a call from a directed call-park slot by dialing a feature access code (FAC) and the number of the call-park slot.

Cisco Unified CME supports Directed Call Park from remote phones, however only phones that are local to the directed call-park slot can retrieve a call.

Park Reservation Groups

Cisco Unified CME 7.1 and later versions allow you to assign ownership to call-park slots by using Park Reservation Groups. A park slot configured with a park reservation group can only be used by phones configured with the same park reservation group. A park slot without a park reservation group can be used by any phone not assigned to a park reservation group.

In versions earlier than Cisco Unified CME 7.1, you could reserve a dedicated call-park slot for a specific phone based on its primary line. All lines on that phone could use the dedicated park slot. The new Park Reservation Group feature in Cisco Unified CME 7.1 provides an enhanced method of reserving park slots that replaces the use of dedicated park slots.

Park reservation groups are not supported for directed call-park slots.

Note The reservation-group is used so that the phone with a reservation group is allowed to park to park-slot(s) within the same reservation group.

Any phone within the same CME can retrieve any parked calls. So the rule is applied when you park the call, not when you retrieve the call.

Dedicated Call-Park Slots

A dedicated, private call-park slot can be configured for an ephone using the **reserved-for** keyword in the **park-slot** command. The dedicated call-park slot is associated with the primary extension of the ephone. All extensions on this phone can park calls in the dedicated park slot. The extensions on this phone are the only extensions that can park a call in the dedicated park slot. Only one call at a time can be parked in a park slot; a busy tone is returned to any attempt to park a call in a slot that is already in use.

Calls can be parked in dedicated call-park slots using any of the following methods (the extension doing the parking must be on a phone whose primary extension is associated with a dedicated park slot).

- With an active call, an IP phone user presses the Park soft key.
- With an active call, an IP phone user presses the Transfer soft key and a standard or custom FAC (feature access code) for the call-park feature. The standard FAC for call park is **6.
- With an active call, an analog phone user presses hookflash and the standard or custom FAC for the call park feature.

Calls can be retrieved from dedicated call-park slots using any of the following methods:

- An IP phone user presses the Pickup soft key and dials the park-slot number.
- An IP phone user presses the New Call soft key and dials the park-slot number.
- An analog phone user lifts the handset, presses the standard or custom FAC for directed call pickup, and dials the park-slot number. The standard FAC for directed pickup is **5.

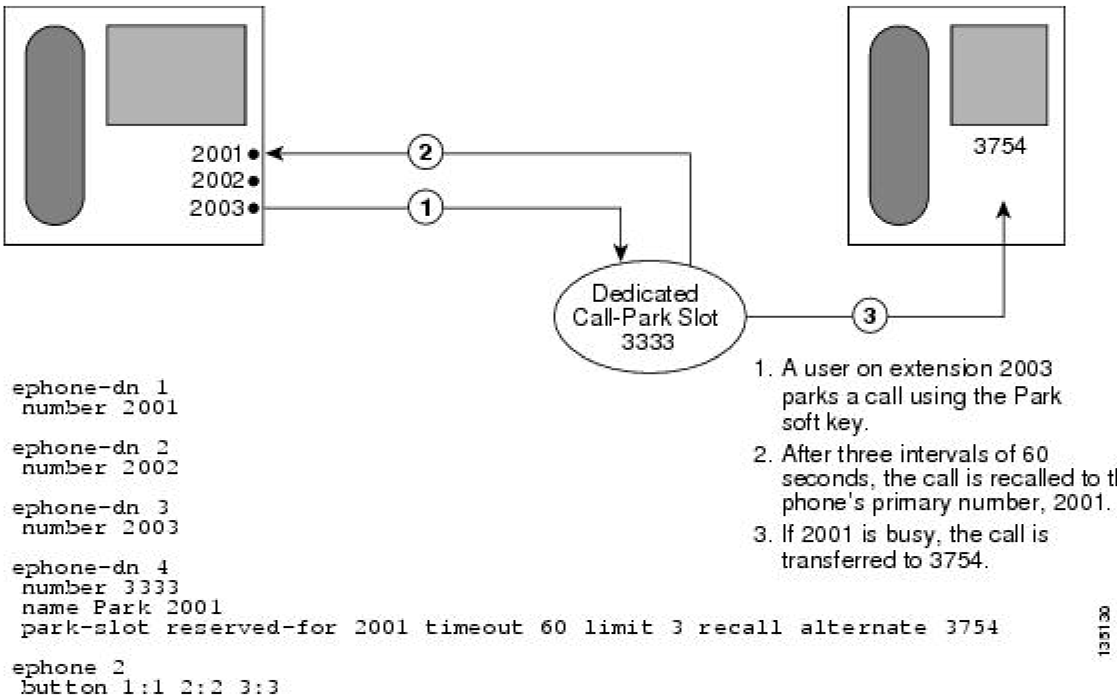
If no dedicated park slot is found anywhere in the Cisco Unified CME system for an ephone-dn that is attempting to park a call, the system uses the standard call-park procedure; that is, the system searches for a preferred park slot (one with an ephone-dn number that matches the last two digits of the ephone-dn attempting to park the call) and if none is found, uses any available call-park slot.

Figure 39: Dedicated Call Park Example, on page 1087 shows an example of a dedicated call-park slot.

If the configuration specifies that a call should be recalled to the parking phone after the timeout intervals expire, the call is always returned to the phone's primary extension number, regardless of which extension on the phone did the parking. Figure 39: Dedicated Call Park Example, on page 1087 shows an ephone that is configured with the extension numbers 2001, 2002, and 2003, and a private call-park slot at extension 3333. The private park slot has been set up to recall calls to the parking phone when the parked call's timeouts expire. In the example, extension 2003 parks a call using the Park soft key. When the timeout intervals expire, the call rings back on extension 2001.

The configuration in Figure 39: Dedicated Call Park Example, on page 1087 specifies that the call will recall or transfer from the park slot after 3 times the 60-second timeout, or after 180 seconds. Also, before the exhaustion of the 3 timeouts the phone will receive reminder notifications that a parked call is waiting. The reminders are sent after each 60-second timeout interval expires (that is, at 60 seconds and at 120 seconds). You may want to set the **timeout** command with a limit of 1 instead, so that the call simply parks and recalls or transfers without sending a reminder ring.

Figure 39: Dedicated Call Park Example



Call-Park Blocking

In Cisco Unified CME 4.0 and later versions, individual ephones can be prevented from making transfers to call-park slots by using the **transfer-park blocked** command. This command prevents transfers to park that use the Transfer soft key and a call-park slot number, while allowing call-parks that use only the Park soft key. (To prevent use of the Park soft key, use an ephone template to remove it from the phone. See Customize Softkeys, on page 925.)

An exception is made for phones with reserved, or dedicated, park slots. If the **transfer-park blocked** command is used on an ephone that has a dedicated park slot, the phone is blocked from parking calls at park slots other than the phone's dedicated park slot but can still park calls at its own dedicated park slot.

Call-Park Redirect

By default, H.323 and SIP calls that use the call-park feature use hairpin call forwarding or transfer to park calls and to pick up calls from park. The **call-park system redirect** command allows you to specify that these calls should use H.450 or the SIP Refer method of call forwarding or transfer. The **no** form of the command returns the system to the default behavior.

Call Park Recall Enhancement

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

In Cisco Unified CME 9.5, the **recall force** keyword is added to the **call-park system** command in telephony-service configuration mode to allow a user to force the recall or transfer of a parked call to the phone that put the call in park or the phone with the reserved-for number as its primary DN when the destination phone is available to answer the call. For more configuration examples, see Example for Configuring Call Park Recall, on page 1098.

Prior to Cisco Unified CME 10.5, the ring tones for park recall and incoming calls were the same. In Cisco Unified CME 10.5, a new ring tone is introduced for park recall to assist the user to distinctly identify the type of call.

This feature is supported on all phone families for SCCP endpoints and on 89XX and 99XX phone families for SIP endpoints. No configurations are required to activate this feature. The ringtone for SCCP endpoints is a feature-ring and for SIP endpoints the ringtone is a Bellcore-dr2.

Park Monitor

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

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

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

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

Configure Call Park

Enable Call Park or Directed Call Park

To enable Call Park on SCCP or SIP phones, perform the following steps.

Restriction

- For SIP phones, the Park soft key is not supported for Cisco Unified IP Phone 7905, 7912, 7921, 7940, or 7960.
- Park Retrieval is supported only on local phones. Phones can park calls remotely to another Cisco Unified CME router but only phones that are registered to the local router hosting the call-park slots can retrieve a call.
- In versions earlier than Cisco Unified CME 7.1, Call Park and Directed Call Park shared the same call-park slots. In Cisco Unified CME 7.1 and later versions, if a user attempts to transfer a call to a basic park slot when using Directed Call Park, Cisco Unified CME considers that a Park Retrieval.
- A user can retrieve a parked call on an SCCP phone by pressing the PickUp soft key and dialing the extension number of the call-park slot or an asterisk (*) only if the **service directed-pickup** command is enabled (default). Otherwise this initiates a local group pickup.
- Park Reservation Groups are not supported with Directed Call Park.
- Different directory numbers with the same extension number must have the same Call Park configuration.
- Calls from H.323 trunks are not supported on SIP phones.
- Hold Pickup is not supported with the **call-park system application** command.

Before You Begin

- SIP phones require Cisco Unified CME 7.1 or a later version.
- IP phone must support the Park soft key. The Park soft key displays by default on supported SCCP and SIP phones. If previously disabled, you must use the **softkeys connected** command to enable the Park soft key.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **call-park system**{**application** |**redirect** }
5. **fac**{**standard** | **custom dpark-retrieval** *custom-fac*}
6. **exit**
7. **ephone-dn** *dn-tag* [**dual-line**]
8. **number** *number* [**secondary** *number*] [**no-reg**[**both**| **primary**]]
9. **park-slot** [**directed**] [**reservation-group** *group-number*] [**reserved-for** *extension-number*] [[**timeout** *seconds***limit** *count*][**notify** *extension-number* [**only**]] [**recall**][**transfer** *extension-number*][**alternate** *extension-number*] [**retry** *seconds***limit** *count*]]
10. **exit**
11. **ephone** *phone-tag* or **voice register pool** *phone-tag*
12. **park reservation-group** *group-number*
13. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**call-park system**{**application** |**redirect** } **Example:** `Router(config-telephony)# call-park system application`	Defines system parameters for the Call Park feature. • **application—**Enables the Call Park and Directed Call Park features supported in Cisco Unified CME 7.1 and later versions. • **redirect—**Specifies that H.323 and SIP calls use H.450 or the SIP Refer method of call forwarding or transfer to park calls and pick up calls from park.
Step 5	**fac**{**standard** | **custom dpark-retrieval** *custom-fac*}	Enables standard FACs or creates a custom FAC or alias for the Directed Park Retrieval feature on SCCP and SIP phones.

	Command or Action	Purpose
	Example: `Router(config-telephony)# fac custom dpark-retrieval #25`	• Enable this command to use the Directed Park Retrieval feature in Cisco Unified CME 7.1 and later versions. • **standard—**Enables standard FACs for all phones. Standard FAC for Park Retrieval is **10. • **custom—**Creates a custom FAC for a feature. • *custom-fac*—User-defined code to dial using the keypad on an IP or analog phone. Custom FAC can be up to 256 characters and contain numbers 0 to 9 and * and #.
Step 6	**exit** **Example:** `Router(config-telephony)# exit`	Returns to privileged EXEC mode.
Step 7	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 1`	Enters ephone dn configuration mode to define a directory number for an IP phone, intercom line, voice port, or a message-waiting indicator (MWI). • *dn-tag*—identifies a particular directory number during configuration tasks. Range is 1 to the maximum number of directory numbers allowed on the router platform. Type ? to display the range.
Step 8	**number** *number* [**secondary** *number*] [**no-reg**[**both**| **primary**]] **Example:** `Router(config-ephone-dn)# number 3001`	Associates an extension number with this directory number. • *number*—String of up to 16 digits that represents an extension or E.164 telephone number. **Note** The primary number must be unique for call-park slots.
Step 9	**park-slot** [**directed**] [**reservation-group** *group-number*] [**reserved-for** *extension-number*] [[**timeout** *seconds***limit** *count*][**notify** *extension-number* [**only**]] [**recall**][**transfer** *extension-number*][**alternate** *extension-number*] [**retry** *seconds***limit** *count*]] **Example:** `Router(config-ephone-dn)# park-slot directed`	Creates an extension (call-park slot) at which calls can be temporarily held (parked). • **directed—**(Optional) Enables Directed Call Park using this extension. This keyword is supported in Cisco Unified CME 7.1 and later versions. • **reservation-group***group-number* **—**(Optional) Reserves this slot for phones configured with the specified reservation group. This is the group assigned to the phone in Step 12. This keyword is supported in Cisco Unified CME 7.1 and later versions. • **reserved-for***extension-number* **—**(Optional) Reserves this slot as a private park-slot for the phone with the specified extension number as its primary line.

	Command or Action	Purpose
		Note The **reservation-group** and **reserved-for** keywords are mutually exclusive. If you use the **reservation-group** keyword, the **reserved-for** keyword is ignored. The reservation-group is used so that the phone with a reservation group is allowed to park to park-slot(s) within the same reservation group. Any phone within the same CME can retrieve any parked calls. So the rule is applied when you park the call, not when you retrieve the call.
Step 10	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits configuration mode.

Step 11	**ephone** *phone-tag* or **voice register pool** *phone-tag*
	
	Example:
	`Router(config)# ephone 1`
	or
	`Router(config)# voice register pool 1`
		Enters ephone configuration mode to set phone-specific parameters for an SCCP phone.
		or
		Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
		• *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type ? to display range.

Step 12	**park reservation-group** *group-number*
	
	Example:
	`Router(config-ephone)# park reservation-group 1`
	or
	`Router(config-register-pool)# park reservation-group 1`
		(Optional) Assigns a call-park reservation group to a phone.
		• *group-number*—Unique number that identifies the reservation group. String can contain up to 32 digits.
		• This command can also be configured in ephone-template or voice register template configuration mode and applied to one or more phones. The phone configuration has priority over the template configuration.
		• This command is supported in Cisco Unified CME 7.1 and later versions.

Step 13	**end**
	
	Example:
	`Router(config-ephone)# end`
	or
	`Router(config-register-pool)# end`
		Exits configuration mode.

Examples for Basic Call Park, Directed Call Park and Park Reservation Groups

Basic Call Park

The following example shows three basic call-park slots that can be used by either SCCP or SIP phones. Any phone can retrieve calls parked at these extensions.

```
ephone-dn  23
 number 8123
 park-slot timeout 10 limit 2 recall
 description park slot for Sales
!
ephone-dn  24
 number 8124
 park-slot timeout 10 limit 2 recall
 description park slot for Sales
!
ephone-dn  25
 number 8125
 park-slot timeout 15 limit 3 recall retry 10 limit 2
 description park slot for Service
```

Directed Call Park

The following example shows that the enhanced Call Park and Directed Call Park features in Cisco Unified CME 7.1 and later versions is enabled with the **call-park system application** command in telephony-service configuration mode. Two call-park slots, extension 3110 and 3111, can be used to park calls for the pharmacy using Directed Call Park.

```
telephony-service
 load 7960-7940 P00308000500
 max-ephones 100
 max-dn 240
 ip source-address 10.7.0.1 port 2000
 cnf-file location flash:
 cnf-file perphone
 voicemail 8900
 max-conferences 8 gain -6
 call-park system application
 transfer-system full-consult
 fac standard
 create cnf-files version-stamp 7960 Sep 25 2007 21:25:47
!
!
ephone-dn  10
 number 3110
 park-slot directed
 description park-slot for Pharmacy
!
ephone-dn  11
 number 3111
 park-slot directed
 description park-slot for Pharmacy
```

Park Reservation Groups

The following example shows park reservation groups set up for two call-park slots. Extension 8126 is configured for group 1 and assigned to phones 3 and 4. Extension 8127 is configured for group 2 and assigned to phones 10 and 11. When calls for the Pharmacy are parked at extension 8126, only phones 3 and 4 can retrieve them.

```
ephone-dn  26
 number 8126
 park-slot reservation-group 1 timeout 15 limit 2 transfer 8100
 description park slot for Pharmacy
!
ephone-dn  27
 number 8127
 park-slot reservation-group 2 timeout 15 limit 2 transfer 8100
 description park slot for Auto
```

```
!
!
ephone  3
 park reservation-group 1
 mac-address 002D.264E.54FA
 type 7962
 button  1:3
!
!
ephone  4
 park reservation-group 1
 mac-address 0030.94C3.053E
 type 7962
 button  1:4
!
!
ephone  10
 park reservation-group 2
 mac-address 00E1.CB13.0395
 type 7960
 button  1:10
!
!
ephone  11
 park reservation-group 2
 mac-address 0016.9DEF.1A70
 type 7960
 button  1:11
```

Verify Call Park

Step 1 Use the **show running-config** command to verify your configuration. Call-park slots are listed in the ephone-dn portion of the output.

Example:

```
Router# show running-config

!
ephone-dn  23
 number 853
 park-slot timeout 10 limit 1 recall
 description park slot for Sales
!
!
ephone-dn  24
 number 8126
 park-slot reserved-for 126 timeout 10 limit 1 transfer 8145
!
!
ephone-dn  25
 number 8121 secondary 121
 park-slot reserved-for 121 timeout 30 limit 1 transfer 8145
!
!
ephone-dn  26
 number 8136 secondary 136
 park-slot reserved-for 136 timeout 10 limit 1 recall
!
!
ephone-dn  30  dual-line
 number 451 secondary 501
 preference 10
 huntstop channel
```

```
!
!
ephone-dn  31  dual-line
 number 452 secondary 502
 preference 10
 huntstop channel
!
```

Step 2 Use the **show telephony-service ephone-dn** command to display call park configuration information.

Example:

```
Router# show telephony-service ephone-dn

ephone-dn  26
 number 8136 secondary 136
 park-slot reserved-for 136 timeout 10 limit 1 recall
```

Configure Timeout Duration for Recalled Calls

To set a timeout duration for no response for a recalled call, perform the following steps. This command is also applicable to all IP phones where a call in ringing state if not answered, is automatically disconnected after the timeout duration.

This feature is enabled by default. You must perform this task only if the feature was previously disabled on a phone.

Before You Begin

Cisco Unified CME 10.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone ring timeouts** *seconds*
4. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone ring timeouts** *seconds* **Example:** `Router(config)# ring timeout 25`	Enters a timeout period before disconnecting the call.
Step 4	**exit** **Example:** `Router(config-ephone)# exit`	Exits to privileged EXEC mode.

Example

The following example shows that the ring timeouts command is enabled on phone:

```
ephone-dn 10 dual-line
number 1001
no huntstop
huntstop channel
ephone-dn 11 dual-line
```

Troubleshooting Call Park

Step 1 **show ephone-dn park**

Use this command to display configured call-park slots and their status.

```
Router# show ephone-dn park

DN 50 (1560) park-slot state IDLE
Notify to () timeout 30 limit 10
```

Step 2 Use the **debug ephone** commands to observe messages and states associated with an ephone. For more information, see Cisco Unified CME Command Reference.

Configuration Examples for Call Park

Example for Configuring Basic Call Park

The following example creates a call-park slot with the number 1560. After a call is parked at this number, the system provides 10 reminder rings at intervals of 30 seconds to the extension that parked the call.

```
ephone-dn 50
number 1560
park-slot timeout 30 limit 10
```

Example for Blocking Phone From Using Call Park

The following example prevents ephone 25 and extensions 234, 235, and 236 from parking calls at any call-park slots.

```
ephone-dn 11
 number 234

ephone-dn 12
 number 235

ephone-dn 13
 number 236

ephone 25
 button 1:11 2:12 3:13
 transfer-park blocked
```

The following example sets up a dedicated park slot for the extensions on ephone 6 and blocks transfers to call park from extensions 2977, 2978, and 2979 on that phone. Those extensions can still park calls at the phone's dedicated park slot by using the Park soft key or the Transfer soft key and the FAC for call park.

```
ephone-dn 3
 number 2558
 name Park 2977
 park-slot reserved-for 2977 timeout 60 limit 3 recall alternate 3754

ephone-dn 4
 number 2977

ephone-dn 5
 number 2978

ephone-dn 6
 number 2979

ephone 6
 button 1:4 2:5 3:6
 transfer-park blocked
```

Example for Configuring Call-Park Redirect

The following example specifies that H.323 and SIP calls that are parked should use H.450 or the SIP Refer method to when they are parked or picked up.

```
telephony-service
call-park system redirect
```

Example for Configuring Call Park Recall

The following example shows how to force the recall of a call previously parked when the phone was busy:

```
Router# configure terminal
Router(config)# telephony-service
Router(config-telephony)# call-park system ?
recall       Configure parameters for recall
Router(config-telephony)# call-park system recall ?
force  Force recall for busy call park initiator
Router(config-telephony)# call-park system recall force
```

Where to Go Next

Controlling Use of the Park Soft Key

To block the functioning of the call park (Park) soft key without removing the key display, create and apply an ephone template that contains the **features blocked** command. For more information, see Customize Softkeys, on page 925.

To remove the call park (Park) soft key from one or more phones, create and apply an ephone template that contains the appropriate **softkeys** command. For more information, see Customize Softkeys, on page 925 .

Ephone Templates

The **transfer-park blocked** command, which blocks transfers to call-park slots, can be included in ephone templates that are applied to individual ephones.

The Park soft key can be removed from the display of one or more phones by including the appropriate **softkeys** command in an ephone template and applying the template to individual ephones.

For more information, see Templates, on page 1427.

Feature Access Codes

You can park calls using a feature access code (FAC) instead of a soft key on the phone if standard or custom FACs have been enabled for your system. The call-park FAC is considered a transfer to a call-park slot and therefore is valid only after the Trnsfer soft key (IP phones) or hookflash (analog phones) has been used to initiate a transfer. The following are the standard FACs for call park:

- Dedicated park slot—Standard FAC is **6.
- Any available park slot—Standard FAC is **6 plus optional park-slot number.

For more information about FACs, see Feature Access Codes, on page 757.

Feature Information for Call Park

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

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

Table 92: Feature Information for Call Park

Feature Name	Cisco Unified CME Version	Feature Information
Call Park Recall Enhancement	9.5	Added recall force keyword to the call-park system command.
Call Park	8.5	Support for Park Monitor was introduced.
	7.1	Adds Call Park support for SIP phones, introduces Park Reservation Groups, and enhances Directed Call Park.
	4.0	Dedicated call-park slots, alternative recall locations, and call-park blocking were introduced. Direct calls to park slots are now interpreted as attempts to pick up parked calls rather than attempts to be parked at the slot.
	3.2.1	Monitoring of call-park slots was introduced.
	3.1	Call park was introduced.

CHAPTER 42

Call Restriction Regulations

Prerequisites for LPCOR

- Cisco IOS Release 15.0(1)XA or a later release.
- Cisco Unified CME 8.0 or a later version.

Information About LPCOR

LPCOR Overview

The Telecom Regulatory Authority of India (TRAI) has regulations that restrict the mixing of voice traffic between the PSTN and VoIP networks. Previously, this required a user to have two phones to handle both PSTN and VoIP calls; an IP phone connected to the Electronic Private Automatic Branch Exchange (EPABX) for intra-office and inter-office VoIP calls and a separate phone connected to a PABX for PSTN calls, as shown in Figure 40: Separate PBX and EPABX Systems, on page 1102.

New regulations allow for a single network infrastructure and single EPABX to connect to both the PSTN and VoIP networks by using a logical partitioning between the PSTN and IP leased lines.

The logical partitioning class of restriction (LPCOR) feature enables a single directory number on an IP phone or analog phone registered to Cisco Unified CME to connect to both PSTN and VoIP calls according to the connection restrictions specified by TRAI regulations. Cisco Unified CME can support both VoIP and PSTN calls while restricting the mixing of voice traffic between the PSTN and VoIP networks and preventing PSTN calls from connecting to remote locations over an IP trunk, as shown in Figure 41: Single EPAPX System with PSTN and VoIP Calls Partitioning, on page 1102.

Figure 40: Separate PBX and EPABX Systems

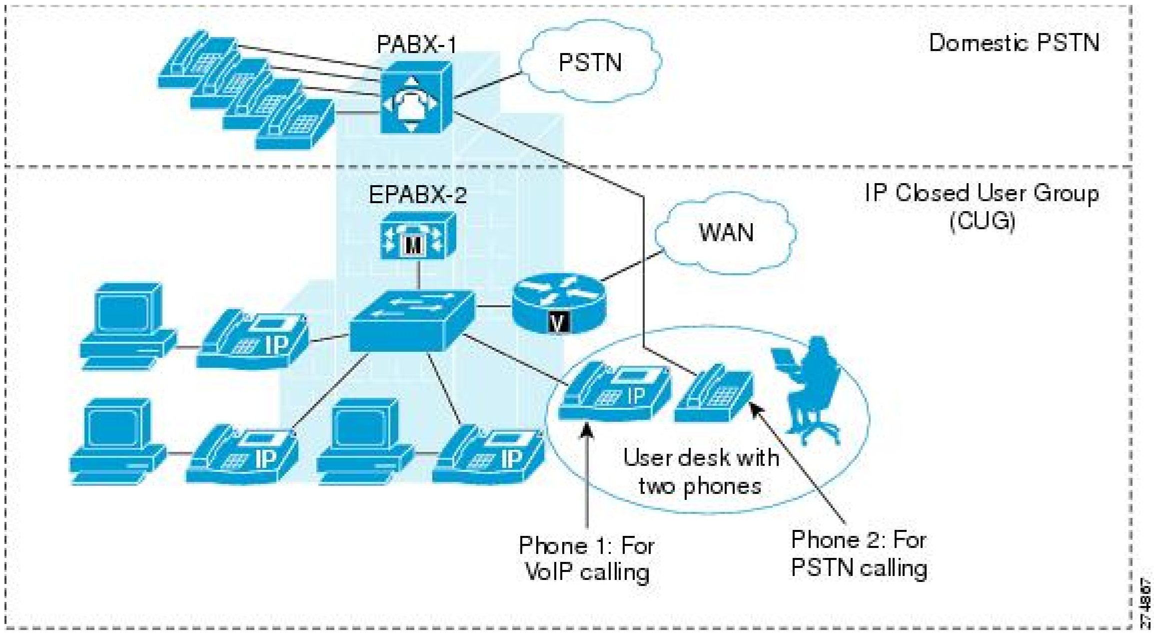
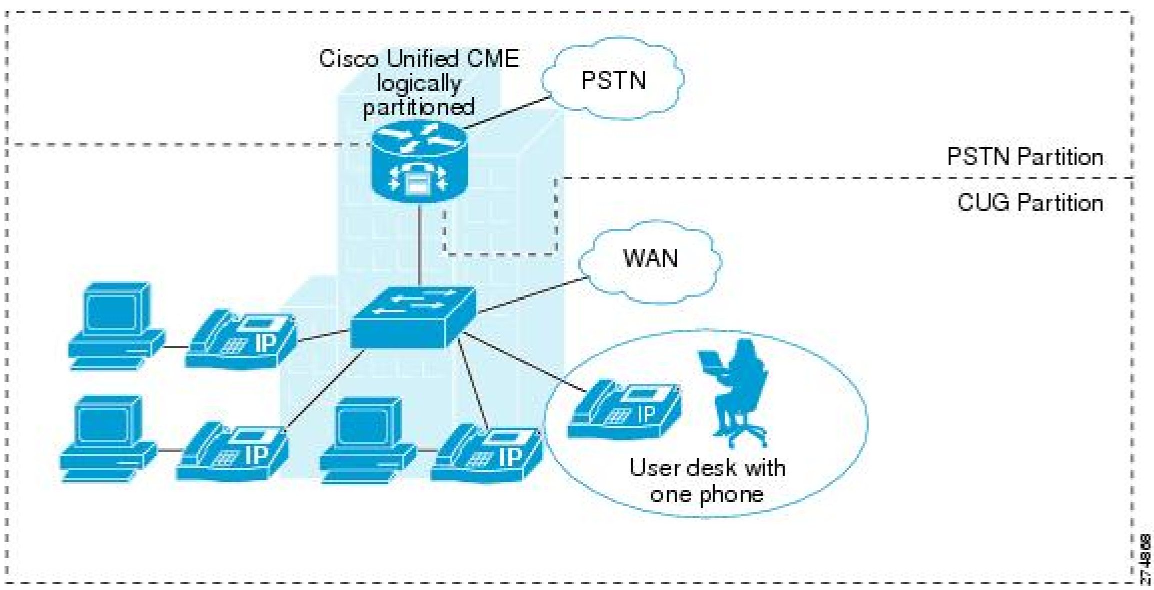


Figure 41: Single EPAPX System with PSTN and VoIP Calls Partitioning



LPCOR Policy and Resource Groups

Cisco Unified CME supports a high-level class of restriction by allowing you to logically partition its resources (PSTN trunks, IP trunks, IP phones, and analog phones) into different groups. The resources of each group are scalable based on the voice interface, trunk group, or IP address subnet. In general, you should not have to modify your existing dial plan to support LPCOR functionality. The dial peer class of restriction (COR) feature remains unchanged when the LPCOR feature is added to Cisco Unified CME.

LPCOR control is based on the location of resources, where calls are originating and terminating. You must partition the resources of the Cisco Unified CME router into different resource groups and then create a LPCOR policy for each group to which you want to apply call restrictions.

You create a LPCOR policy matrix for individual resource groups by defining its LPCOR policy to either accept or reject calls that originate from any of the other resource groups. You can define one LPCOR policy for each resource group.

The same LPCOR policy is applied to multiple directory numbers from the same resource. For example, if multiple directory numbers are defined for a SCCP phone, the same LPCOR policy is enforced for all calls to the different directory numbers on the SCCP phone.

In the following example, PSTN trunks, IP trunks (H.323 and SIP), analog FXS phones, and IP phones for a Cisco Unified CME router are partitioned into five different resource groups (RG1 to RG5).

Table 93: LPCOR Policy Matrix Example

Resource Groups	RG1	RG2	RG3	RG4	RG5
RG1	**Yes**	No	Yes	No	Yes
RG2	Yes	Yes	**No**	Yes	No
RG3	Yes	**Yes**	Yes	Yes	No
RG4	No	No	No	Yes	Yes
RG5	No	Yes	Yes	Yes	**No**

LPCOR validation is done at the target destination based on the configured LPCOR policy matrix. For example:

- Call from RG1 to target RG1 is allowed
- Call from RG2 to target RG3 is not allowed
- Call from RG3 to target RG2 is allowed
- Call from RG5 to target RG5 is not allowed

Default LPCOR Policy

The default LPCOR policy means that there are no restrictions between the call source and its target destination. When a call is presented to a target destination, Cisco Unified CME bypasses LPCOR validation if either the incoming call is not associated with a LPCOR policy or the LPCOR policy is not defined for the target destination.

TRAI regulations allow the same directory number on a local IP phone or SCCP analog Foreign Exchange Station (FXS) phone in Cisco Unified CME to handle both PSTN and VoIP calls. Locally connected phones do not have to be associated with any resource group.

How LPCOR Policies are Associated with Resource Groups

Call restrictions are applied to LPCOR resource groups based on the location of the resources. You create LPCOR policies that define the call restrictions to apply to calls that originate or terminate at the following types of resources.

Analog Phones

TRAI regulations allow an analog FXS phone to accept both PSTN and VoIP calls if the phone is locally registered to Cisco Unified CME. Locally connected phones do not have to be associated with any resource group; the default LPCOR policy is applied to this phone type.

A specific LPCOR policy can be defined through the voice port or trunk group. For configuration information, see Associate a LPCOR Policy with Analog Phone or PSTN Trunk Calls, on page 1114.

IP Phones

LPCOR supports both SCCP and SIP IP phones. TRAI regulations allow an IP phone to accept both PSTN and VoIP calls if the IP phone is registered locally to Cisco Unified CME through the LAN. If the IP phone is registered to Cisco Unified CME through the WAN, PSTN calls must be blocked from the remote IP phones.

If an IP phone always registers to Cisco Unified CME from the same local or remote region, the phone is provisioned with a static LPCOR policy. For configuration information, see Associate a LPCOR Policy with IP Phone or SCCP FXS Phone Calls, on page 1120.

If the phone is a mobile-type IP phone and moves between the local and remote regions, such as an Extension Mobility phone, Cisco IP Communicator softphone, or a remote teleworker phone, the LPCOR policy is provisioned dynamically based on the IP phone's currently registered IP address. For configuration information, see Associate LPCOR with Mobile Phone Calls, on page 1124.

PSTN Trunks

An incoming LPCOR resource group is associated with a PSTN trunk (digital or analog) through the voice port or trunk group.

When a call is routed to the PSTN network, the LPCOR policy of the target PSTN trunk can block calls from any resource group it is not explicitly configured to accept. Outgoing calls from a PSTN trunk are associated with a LPCOR policy based on either the voice port or trunk group, whichever is configured in the outbound POTS dial-peer.

For configuration information, see Associate a LPCOR Policy with Analog Phone or PSTN Trunk Calls, on page 1114.

VoIP Trunks

An incoming VoIP trunk call (H.323 or SIP) is associated with a LPCOR policy based on the remote IP address as follows:

Incoming H.323 trunk call

- IP address of the previous hub or originating gateway

Incoming SIP trunk call

- IP address of the originating gateway
- Hostname from the earliest Via header of an incoming INVITE message. If the hostname is in domain name format, a DNS query is performed to resolve the name into an IP address.

Cisco Unified CME uses the resolved hostname or resolved IP address to determine the LPCOR policy based on the entries in the IP-trunk subnet table. If the LPCOR policy cannot be found through the IP address or hostname, the incoming H.323 or SIP trunk call is associated with the incoming LPCOR policy configured in voice service configuration mode.

The LPCOR policy of the VoIP target is determined through the configuration of the outbound VoIP dial-peer. The default LPCOR policy is applied to the VoIP target if an outgoing LPCOR policy is not defined in the target VoIP dial-peer.

For configuration information, see Associate a LPCOR Policy with VoIP Trunk Calls, on page 1117.

LPCOR Support for Supplementary Services

Table 94: Supplementary Services Support with LPCOR, on page 1105 describes LPCOR support for calls using supplementary services.

Table 94: Supplementary Services Support with LPCOR

Feature	Description	SCCP Phone	SIP Phone
Basic Call	Cisco Unified CME invokes the LPCOR policy validation if both the incoming call and target destination are associated with a LPCOR policy. If the LPCOR policy validation fails, cause-code 63 (no service available) or the user-defined cause-code is returned to the remote switch. The call can hunt to the next destination.	Yes	Yes

Feature	Description	SCCP Phone	SIP Phone
Call Forward	When a call is forwarded to a new destination, Cisco Unified CME invokes the LPCOR policy validation between the source and the forwarding target. The call is not forwarded to the target if the LPCOR policy is restricted.	Yes	Yes
Call Transfer	Blind and Consultative Call Transfer is restricted if the LPCOR policy validation fails between the transferee and transfer-to parties. For consultative call transfers, the reorder tone plays and an error message displays on the transferor phone. The call is not disconnected between the transferee and transferor.	Yes	Yes

<table>
<tr><th>Feature</th><th>Description</th><th>SCCP Phone</th><th>SIP Phone</th></tr>
<tr><td>Ad Hoc Conference (software-based, 3-party)</td><td rowspan="2">Cisco Unified CME invokes the LPCOR policy validation for each call joined to a conference. A call is blocked from joining the conference if the LPCOR policy validation fails.

The reorder tone plays and the conference cannot complete message displays on the IP phone that initiated the conference. The call is resumed by the transferor who initiated the conference.

Note If the LPCOR policy validation fails during a blind transfer setup to a conference bridge, the call is released.
Note LPCOR validation is not supported for additional call transfer or conference operations from a 3-party software conference call.</td><td>Yes</td><td>No</td></tr>
<tr><td>Ad Hoc Conference (hardware-based)</td><td>Yes</td><td>Yes</td></tr>
</table>

Feature	Description	SCCP Phone	SIP Phone
Meet-Me Conference	LPCOR policy of each conference party is validated when a new call is joined to a conference. The call is blocked from joining the conference if the LPCOR policy validation fails. The reorder tone plays and the conference cannot complete message displays on the IP phone that initiated the Meet-Me conference.	Yes	Yes (join only)
Call Pickup/Group Pickup (Cisco Unified CME 7.1 and later versions)	Call Pickup and Pickup Groups enable phone users to answer a call that is ringing on a different extension. The pickup is blocked if the LPCOR policy validation between the call and the pickup phone fails. The reorder tone plays and the unknown number message displays on the IP phone that attempts the call pickup.	Yes	Yes
Call Park (Cisco Unified CME 7.1 and later versions)	Phone users can place a call on hold at a special extension so it can be retrieved by other phones.	Yes	Yes
Call Park Retrieval	A phone is not allowed to retrieve a parked call if the LPCOR policy validation fails. The reorder tone plays and the unknown number message displays on the IP phone that attempts to retrieve the parked call. The call remains parked at the call-park slot.	Yes	Yes

Feature	Description	SCCP Phone	SIP Phone
Hunt Group Pilot (ephone hunt group)	Supported for sequential and longest idle hunt groups. The LPCOR policy validation is performed when a call is directed to a SCCP endpoint through the ephone hunt-group.	Yes	No
Hunt Group Pilot (voice hunt group)	Supported for parallel hunt groups only. A hunt target can be a SCCP phone, SIP phone, VoIP trunk, or PSTN trunk. The LPCOR policy validation is performed between the call and the pilot hunt target. A call is blocked from a target if the LPCOR policy is restricted.	Yes	Yes
Shared Line	Phones with a shared directory number must have the same LPCOR policy.	Yes	Yes
CBarge	Phone users who share a directory number can join an active call on the shared line. Phones must have the same LPCOR policy.	Yes	Yes
Third-Party Call Control	Cisco Unified CME supports out-of-dialog refer (OOD-R) by a remote call-control system. The LPCOR validation is performed during the second outbound call setup after the first outbound call is established. The OOD-R request fails if the LPCOR policy between the first and second outbound call is restricted.	Yes	Yes

Phone Display and Warning Tone for LPCOR

Cisco Unified CME plays the reorder tone to callers when it blocks calls due to LPCOR policy authentication. Table 95: Message Display for Blocked LPCOR Calls, on page 1110 lists the message that displays on the phone when a call is blocked.

Table 95: Message Display for Blocked LPCOR Calls

Call Block Type	Phone Display Message	
	SCCP Phone	**SIP Phone**
Call Transfer	Unable to Transfer	Transfer Failed
Conference	Cannot Complete Conference	
Meet-Me Conference	No Screen Display Update	
Pickup	Unknown Number	
Park	Unknown Number	

LPCOR VSAs

New vendor-specific attributes (VSAs) for the LPCOR policy associated with a call are included in the call detail records (CDRs) generated by Cisco Unified CME for Remote Authentication Dial-in User Services (RADIUS) accounting. A null value is used for call legs without an associated LPCOR policy, which is the default LPCOR value. The incoming or outgoing LPCOR policy of a call is added to RADIUS stop records.

Table 96: VSAs Supported by Cisco Voice Calls , on page 1111lists the new VSAs.

Table 96: VSAs Supported by Cisco Voice Calls

Attribute	VSA No. (Decimal)	Format for Value or Text	Sample Value or Text	Description
in-lpcor-group	1	String	`pstn_group`	Logical partitioning class of restriction (LPCOR) resource-group policy associated with an incoming call.
out-lpcor-group	1	String	`voip_group`	LPCOR resource-group policy associated with an outgoing call.

Configure LPCOR

Define a LPCOR Policy

To enable LPCOR functionality and define a policy for each resource group that requires call restrictions, perform the following task. You can define one LPCOR policy for each resource group. Do not create a LPCOR policy for resource groups that do not require call restrictions. A target resource group without a LPCOR policy can accept incoming calls from any other resource group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice lpcor enable**
4. **voice lpcor call-block cause** *cause-code*
5. **voice lpcor custom**
6. **group** *number lpcor-group*
7. **exit**
8. **voice lpcor policy** *lpcor-group*
9. **accept** *lpcor-group*
10. **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 lpcor enable** **Example:** `Router(config)# voice lpcor enable`	Enables LPCOR functionality on the Cisco Unified CME router.
Step 4	**voice lpcor call-block cause** *cause-code* **Example:** `Router(config)# voice lpcor call-block cause 79`	(Optional) Defines the cause code to use when a call is blocked because LPCOR validation fails. • Range: 1 to 180. Default: 63 (serv/opt-unavail-unspecified). Type **?** to display a description of the cause codes.
Step 5	**voice lpcor custom** **Example:** `Router(config)# voice lpcor custom`	Defines the name and number of LPCOR resource groups on the Cisco Unified CME router.
Step 6	**group** *number lpcor-group* **Example:** `Router(cfg-lpcor-custom)# group 1 pstn_trunk`	Adds a LPCOR resource group to the custom resource list. • *number*—Group number of the LPCOR entry. Range: 1 to 64. • *lpcor-group*—String that identifies the LPCOR resource group.
Step 7	**exit** **Example:** `Router(cfg-lpcor-custom)# exit`	Exits LPCOR custom configuration mode.
Step 8	**voice lpcor policy** *lpcor-group* **Example:** `Router(config)# voice lpcor policy pstn_trunk`	Creates a LPCOR policy for a resource group. • *lpcor-group*—Name of the resource group that you defined in Step 6.

	Command or Action	Purpose
Step 9	**accept** *lpcor-group* **Example:** `Router(cfg-lpcor-policy)# accept analog_phone`	Allows a LPCOR policy to accept calls associated with the specified resource group. • Default: Calls from other groups are rejected; calls from the same resource group are accepted. • Repeat this command for each resource group whose calls you want this policy to accept.
Step 10	**end** **Example:** `Router(cfg-lpcor-policy)# end`	Returns to privileged EXEC mode.

Examples

The following example shows a LPCOR configuration where resources are partitioned into five groups. Three of the resource groups have LPCOR policies that limit the calls they can accept. The other two groups, ipphone_local and analog_phone, can accept calls from any of the other resource groups because they do not have a LPCOR policy defined.

```
voice lpcor enable
voice lpcor call-block cause invalid-number
voice lpcor custom
 group 1 pstn_trunk
 group 2 analog_phone
 group 3 iptrunk
 group 4 ipphone_local
 group 5 ipphone_remote
!
voice lpcor policy pstn_trunk
 accept analog_phone
 accept ipphone_local
!
voice lpcor policy iptrunk
 accept analog_phone
 accept ipphone_local
 accept ipphone_remote
!
voice lpcor policy ipphone_remote
 accept iptrunk
 accept analog_phone
 accept ipphone_local
```

The following example shows a LPCOR configuration where resources are partitioned into the following four policy groups:

- siptrunk—Accepts all IP trunk calls.
- h323trunk—Accepts all IP trunk calls.
- pstn—Blocks all IP trunk and voice-mail calls.

- voicemail—Accepts both IP trunk and PSTN calls.

```
voice lpcor enable
voice lpcor custom
 group 1 siptrunk
 group 2 h323trunk
 group 3 pstn
 group 4 voicemail
!
voice lpcor policy siptrunk
 accept h323trunk
 accept voicemail
!
voice lpcor policy h323trunk
 accept siptrunk
 accept voicemail
!
voice lpcor policy pstn
!
voice lpcor policy voicemail
 accept siptrunk
 accept h323trunk
 accept pstn
```

The following example shows a LPCOR policy that is configured to reject calls associated with itself. Devices that belong to the local_phone resource group cannot accept calls from each other.

```
voice lpcor policy local_phone
 no accept local_phone
 accept analog_phone
```

Associate a LPCOR Policy with Analog Phone or PSTN Trunk Calls

To associate a LPCOR policy with calls that originate or terminate at an analog phone or PSTN trunk, perform the following task. You can apply a specific LPCOR policy through the voice port or trunk group to remote analog phones or to local analog phones that you do not want to associate with the default LPCOR policy.

Note For an analog FXS phone that is locally registered to Cisco Unified CME through the LAN, see Associate a LPCOR Policy with IP Phone or SCCP FXS Phone Calls, on page 1120.

Incoming calls from an analog phone or PSTN trunk are associated with a LPCOR resource group based on the following configurations, in the order listed:

1. Voice port
2. Trunk group

Outgoing calls from an analog phone or PSTN trunk are associated with a LPCOR policy based on the voice port or trunk group configuration in the outbound POTS dial-peer:

- If the outbound dial peer is configured with the **port** command, an outgoing call uses the LPCOR policy specified in the voice port.
- If the outbound dial-peer is configured with the **trunkgroup** command, the call uses the LPCOR policy specified in the trunk group.

Before You Begin

The LPCOR policy must be defined. See Define a LPCOR Policy, on page 1111.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **trunk group** *name*
4. **lpcor incoming** *lpcor-group*
5. **lpcor outgoing** *lpcor-group*
6. **exit**
7. **voice-port** *port*
8. **lpcor incoming** *lpcor-group*
9. **lpcor outgoing** *lpcor-group*
10. **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	**trunk group** *name* **Example:** `Router(config)# trunk group isdn1`	Enters trunk-group configuration mode to define a trunk group.
Step 4	**lpcor incoming** *lpcor-group* **Example:** `Router(config-trunk-group)# lpcor incoming isdn_group1`	Associates a LPCOR resource-group policy with an incoming call.
Step 5	**lpcor outgoing** *lpcor-group* **Example:** `Router(config-trunk-group)# lpcor outgoing isdn_group1`	Associates a LPCOR resource-group policy with an outgoing call.
Step 6	**exit**	

	Command or Action	Purpose
	Example: `Router(config-trunk-group)# exit`	
Step 7	**voice-port** *port* **Example:** `Router(config)# voice-port 0/1/0`	Enters voice-port configuration mode. • *Port* argument is platform-dependent; type **?** to display syntax.
Step 8	**lpcor incoming** *lpcor-group* **Example:** `Router(config-voiceport)# lpcor incoming vp_group3`	Associates a LPCOR resource-group policy with an incoming call.
Step 9	**lpcor outgoing** *lpcor-group* **Example:** `Router(config-voiceport)# lpcor outgoing vp_group3`	Associates a LPCOR resource-group policy with an outgoing call.
Step 10	**end** **Example:** `Router(config-voiceport)# end`	Returns to privileged EXEC mode.

Examples for Configuring LPCOR for a PSTN Trunk and Analog Phones

PSTN Trunks

The following example shows a configuration for a PSTN trunk. Outbound calls from dial peer 201 use LPCOR policy isdn_group1 because dial peer 201 is configured with trunk group isdn1. Outbound calls from dial peer 202 use LPCOR policy vp_group3 because dial peer 202 is configured with voice port 3/1:15. A dial peer can be configured with either a voice port or trunk group; it cannot use both.

```
trunk group isdn1
 lpcor incoming isdn_group1
 lpcor outgoing isdn_group1
!
interface Serial2/0:15
 isdn incoming-voice voice
 trunk-group isdn1
...
voice-port 3/1:15
 lpcor incoming vp_group3
 lpcor outgoing vp_group3
!
!
dial-peer voice 201 pots
description TG outbound dial-peer
destination-pattern 201T
trunkgroup isdn1
```

```
!
dial-peer voice 202 pots
description VP outbound dial-peer
destination-pattern 202T
port 3/1:15
```

Analog Phones

The following example shows a LPCOR configuration for analog phones:

```
trunk group analog1
 lpcor incoming analog_group1
 lpcor outgoing analog_group1
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
 lpcor incoming vp_group1
 lpcor outgoing vp_group1
!
dial-peer voice 100 pots
 description VP dial-peer
 destination-pattern 100
 port 1/0/0
!
dial-peer voice 101 pots
 description VP dial-peer
 destination-pattern 101
 port 1/0/1
!
dial-peer voice 110 pots
 description VP dial-peer
 destination-pattern 110
 port 1/1/0
!
dial-peer voice 300 pots
 description TG outbound dial-peer
 destination-pattern 300
 trunk-group analog1
```

Associate a LPCOR Policy with VoIP Trunk Calls

To associate a LPCOR policy with calls that originate or terminate at a VoIP trunk (H.323 or SIP), perform the following task.

Incoming VoIP trunk calls are associated with a LPCOR policy based on the following configurations, in the order listed:

1. IP-trunk subnet table
2. Voice service voip configuration

Outgoing VoIP trunk calls are associated with a LPCOR policy based on the following configurations, in the order listed:

1. Outbound VoIP dial peer
2. Default LPCOR policy (no LPCOR policy is applied)

Restriction

- The LPCOR IP-trunk subnet table is not supported for calls with an IPv6 address. The LPCOR policy specified with the **lpcor incoming** command in voice service configuration mode is supported for IPv6 trunk calls.
- Only a single LPCOR policy is applied to outgoing IP trunk calls if the outbound VoIP dial-peer is configured with the **session target** command using the **sip-server** or **ras** keyword.
- If a dial peer COR and LPCOR are both defined in a dial peer, the dial peer COR configuration has priority over LPCOR. For example, if the dial peer COR restricts the call and LPCOR allows the call, the call fails because of the dial peer COR before ever considering LPCOR.

Before You Begin

The LPCOR policy must be defined. See Define a LPCOR Policy, on page 1111.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice lpcor ip-trunk subnet incoming**
4. **index** *index-number lpcor-group* {*ipv4-address network-mask* | **hostname** *hostname*}
5. **exit**
6. **voice service voip**
7. **lpcor incoming** *lpcor-group*
8. **exit**
9. **dial-peer voice** *tag* **voip**
10. **lpcor outgoing** *lpcor-group*
11. **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.

	Command or Action	Purpose
Step 3	**voice lpcor ip-trunk subnet incoming** **Example:** `Router(config)# voice lpcor ip-trunk subnet incoming`	Creates a LPCOR IP-trunk subnet table for incoming calls from a VoIP trunk.
Step 4	**index** *index-number lpcor-group* {*ipv4-address network-mask* | **hostname** *hostname*} **Example:** `Router(cfg-lpcor-iptrunk-subnet)# index 1 h323_group1 172.19.33.0 255.255.255.0`	Adds a LPCOR resource group to the IP trunk subnet table.
Step 5	**exit** **Example:** `Router(cfg-lpcor-iptrunk-subnet)# exit`	Exits LPCOR custom configuration mode.
Step 6	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode to specify the VoIP encapsulation type.
Step 7	**lpcor incoming** *lpcor-group* **Example:** `Router(conf-voi-serv)# lpcor incoming voip_trunk_1`	Associates a LPCOR resource-group policy with an incoming call.
Step 8	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits voice-service configuration mode.
Step 9	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 233 voip`	Enters dial-peer configuration mode to define a dial peer for VoIP calls.
Step 10	**lpcor outgoing** *lpcor-group* **Example:** `Router(config-dial-peer)# lpcor outgoing h323_group1`	Associates a LPCOR resource-group policy with an outgoing call.
Step 11	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Examples

The following example shows a LPCOR configuration for VoIP trunks:

```
voice lpcor ip-trunk subnet incoming
 index 1 h323_group1 172.19.33.0 255.255.255.0
 index 2 sip_group1 172.19.22.0 255.255.255.0
 index 3 sip_group2 hostname sipexample
!
voice service voip
 lpcor incoming voip_trunk_1
!
dial-peer voice 233 voip
 description H323 trunk outbound dial-peer
 destination-pattern 233T
 session target ipv4:172.19.33.233
 lpcor outgoing h323_group1
!
dial-peer voice 2255 voip
 description SIP trunk outbound dial-peer
 destination-pattern 255T
 session protocol sipv2
 session target ipv4:172.19.33.255
 lpcor outgoing sip_group1
```

Associate a LPCOR Policy with IP Phone or SCCP FXS Phone Calls

To associate a LPCOR policy with calls that originate or terminate at a local or remote IP phone or local SCCP analog (FXS) phone, perform the following task.

According to TRAI requirements, an IP phone or a SCCP FXS phone can accept both PSTN and VoIP calls if it is locally registered to Cisco Unified CME through the LAN. If a phone is registered to Cisco Unified CME through the WAN, then PSTN calls must be blocked from that remote phone.

Restriction

- Phones that share a directory number must be configured with the same LPCOR policy. A warning message displays if you try to configure a different LPCOR policy between IP phones that share the same directory number.
- Local and remote IP phones cannot use the same LPCOR policy.
- Software-based three-party ad hoc conferencing is not supported on SIP phones.
- Hardware-based ad hoc conferening is not supported on SIP phones.
- LPCOR feature is not supported on voice gateways such as the Cisco VG224 or Cisco integrated service router if the voice gateway is registered to Cisco Unified Communications Manager. Cisco Unified Communications Manager does not support LPCOR.
- If a third-party call-control application makes two separate calls to Cisco Unified CME and performs a media bridging between the two calls, LPCOR validation is not supported because Cisco Unified CME is not aware of the bridging.

Before You Begin

- The LPCOR policy must be defined. See Define a LPCOR Policy, on page 1111.
- SCCP FXS phones are configured with the **type anl** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag* or **voice register pool** *phone-tag*
4. **lpcor type**{**local** | **remote**}
5. **lpcor incoming** *lpcor-group*
6. **lpcor outgoing** *lpcor-group*
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	**ephone** *phone-tag* or **voice register pool** *phone-tag*
	
	Example:
	`Router(config)# ephone 2`
	or
	`Router(config)# voice register pool 4`
		Enters ephone configuration mode to set phone-specific parameters for an SCCP phone.
		or
		Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
		• *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range.

Step 4	**lpcor type**{**local** | **remote**}
	
	Example:
	`Router(config-ephone)# lpcor type remote`
	or
	`Router(config-register-pool)# lpcor type local`
		Sets the LPCOR type for an IP phone.
		• **local**—IP phone always registers to Cisco Unified CME through the LAN.
		• **remote**—IP phone always registers to Cisco Unified CME through the WAN.
		• This command can also be configured in ephone-template or voice register template configuration mode and applied to one or more phones. The phone configuration has precedence over the template configuration.

Step 5	**lpcor incoming** *lpcor-group*	Associates a LPCOR resource-group policy with an incoming call.

	Command or Action	Purpose

	Example:
	`Router(config-ephone)# lpcor incoming ephone_group1`
	or
	`Router(config-register-pool)# lpcor incoming remote_group3`
		• If this phone shares a directory number with another phone, you cannot configure a LPCOR policy that is different than the LPCOR policy on the other phone.
		• This command can also be configured in ephone-template or voice register template configuration mode and applied to one or more phones. The phone configuration has precedence over the template configuration.

Step 6	**lpcor outgoing** *lpcor-group*
	Example:
	`Router(config-ephone)# lpcor outgoing ephone_group2`
	or
	`Router(config-register-pool)# lpcor outgoing remote_group3`
		Associates a LPCOR resource-group policy with an outgoing call.
		• If this phone shares a directory number with another phone, you cannot configure a LPCOR policy that is different than the LPCOR policy on the other phone.
		• This command can also be configured in ephone-template or voice register template configuration mode and applied to one or more phones. The phone configuration has precedence over the template configuration.

Step 7	**end**
	Example:
	`Router(config-ephone)# end`
	or
	`Router(config-register-pool)# end`
		Returns to privileged EXEC mode.

Example for Configuring LPCOR on SCCP Phone, SIP Phones, and SCCP FXS Phones

SCCP

The following example shows a LPCOR configuration for two SCCP phones. One configuration is applied directly to the phone and the other is applied through a phone template:

```
ephone-template 1
 lpcor type local
 lpcor incoming ephone_group1
 lpcor outgoing ephone_group1
!
ephone 1
 mac-address 00E1.CB13.0395
 ephone-template 1
 type 7960
 button 1:1
!
ephone 2
 lpcor type remote
 lpcor incoming ephone_group2
 lpcor outgoing ephone_group2
 mac-address 001C.821C.ED23
```

```
 type 7960
 button 1:2
```

SIP

The following example shows a LPCOR configuration for two SIP phones:

```
voice register template 1
 lpcor type local
 lpcor incoming test_group
 lpcor outgoing test_group
!
voice register pool 3
 id mac 001B.D584.E80A
 type 7960
 number 1 dn 2
 template 1
 codec g711ulaw
!
voice register pool 4
 lpcor type remote
 lpcor incoming remote_group3
 lpcor outgoing remote_group3
 id mac 0030.94C2.9A55
 type 7960
 number 1 dn 2
 dtmf-relay rtp-nt
```

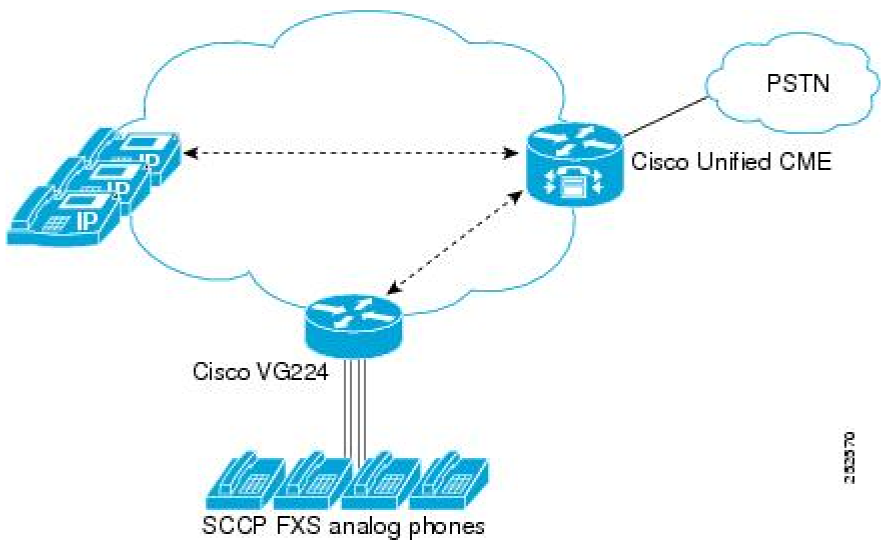
SCCP FXS Analog

The following example shows a LPCOR configuration for two SCCP FXS phones connected to a Cisco VG224 and controlled by Cisco Unified CME:

```
dial-peer voice 102 pots
 service stcapp
 port 1/0/2
!
ephone 5
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2402
 ephone-template 1
 max-calls-per-button 2
 type anl
 button 1:5
!
ephone 6
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2403
 ephone-template 1
 max-calls-per-button 2
 type anl
 button 1:6
```

Figure 42: SCCP FXS Phones Managed by Cisco Unified CME, on page 1124 shows an example of a network with SCCP FXS phones managed by Cisco Unified CME.

Figure 42: SCCP FXS Phones Managed by Cisco Unified CME



Associate LPCOR with Mobile Phone Calls

To associate a LPCOR policy with calls that originate or terminate at a mobile-type phone, perform the following task.

A mobile-type phone can register to Cisco Unified CME through either the LAN or WAN. For example an Extension Mobility phone, Cisco IP Communicator softphone, or a remote teleworker phone.

Incoming and outgoing calls to and from a mobile-type phone are associated with a LPCOR policy based on the following configurations, in the order listed:

1. IP-phone subnet table
2. Default LPCOR policy for mobile-type phones

Restriction The LPCOR IP-phone subnet table is not supported for calls with an IPv6 address.

Before You Begin

The LPCOR policy must be defined. See Define a LPCOR Policy, on page 1111.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag* or **voice register pool** *phone-tag*
4. **lpcor type mobile**
5. **exit**
6. **voice lpcor ip-phone subnet**{**incoming** |**outgoing**}
7. **index** *index-number lpcor-group*{*ipv4-address network-mask* [**vrf***vrf-name*] | **dhcp-pool** *pool-name*}
8. **exit**
9. **voice lpcor ip-phone mobility**{**incoming** | **outgoing**} *lpcor-group*
10. **exit**

DETAILED STEPS

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

Step 3	**ephone** *phone-tag* or **voice register pool** *phone-tag*
	
	Example:
	`Router(config)# ephone 1`
	or
	`Router(config)# voice register pool 1`
		Enters ephone configuration mode to set phone-specific parameters for an SCCP phone.
		or
		Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
		• *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range.

Step 4	**lpcor type mobile** **Example:** `Router(config-ephone)# lpcor type mobile`	Sets the LPCOR type for a mobile-type phone. • This command can also be configured in ephone-template or voice register template configuration mode and applied to one or more phones. The phone configuration has precedence over the template configuration.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-ephone)# exit`	Exits the phone configuration.
Step 6	**voice lpcor ip-phone subnet**{**incoming** |**outgoing**} **Example:** `Router(config)# voice lpcor ip-phone subnet incoming`	Creates a LPCOR IP-phone subnet table for calls to or from a mobile-type phone.
Step 7	**index** *index-number lpcor-group*{*ipv4-address network-mask* [**vrf***vrf-name*] | **dhcp-pool** *pool-name*} **Example:** `Router(cfg-lpcor-ipphone-subnet)# index 1 local_group1 dhcp-pool pool1`	Adds a LPCOR group to the IP-phone subnet table.
Step 8	**exit** **Example:** `Router(cfg-lpcor-ipphone-subnet)# exit`	Exits LPCOR IP-phone configuration mode.
Step 9	**voice lpcor ip-phone mobility**{**incoming** | **outgoing**} *lpcor-group* **Example:** `Router(config)# voice lpcor ip-phone mobility incoming remote_group1`	Sets the default LPCOR policy for mobile-type phones.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Examples

The following example shows the configuration for three mobile-type phones:

```
ephone 270
 lpcor type mobile
 mac-address 1234.4321.6000
 type 7960
 button 1:6
 mtp
 codec g729r8 dspfarm-assist
 description teleworker remote phone
ephone 281
 lpcor type mobile
 mac-address 0003.4713.5554
 type CIPC
 button 1:5
```

```
...
voice register pool 6
 lpcor type mobile
 id mac 0030.94C2.9A66
 type 7960
 number 1 dn 3
 dtmf-relay rtp-nte
```

The following example shows a LPCOR IP-phone subnet configuration with a single shared IP address pool. Any mobile-type IP phones with a shared IP address from DHCP pool1 are considered local IP phones and are associated with the local_group1 LPCOR policy. Other mobile-type IP phones without a shared IP address are considered remote IP phones and are associated with remote_group1, the default LPCOR policy for mobile-type phones.

```
ip dhcp pool pool1
 network 10.0.0.0 255.255.0.0
 option 150 ip 10.0.0.1
 default-router 10.0.0.1
!
!
voice lpcor ip-phone subnet incoming
 index 1 local_group1 dhcp-pool pool1
!
voice lpcor ip-phone subnet outgoing
 index 1 local_group1 dhcp-pool pool1
!
voice lpcor ip-phone mobility incoming remote_group1
 voice lpcor ip-phone mobility outgoing remote_group1
```

The following example shows a LPCOR IP-phone subnet configuration with a separate IP address DHCP pools. Any mobile-type IP phones with separate DHCP pools are considered local IP phones and are assigned the local_group1 LPCOR policy. Other mobile-type IP phones without a DHCP address are considered remote IP phones and are assigned the remote_group1 LPCOR policy.

```
ip dhcp pool client1
 network 10.0.0.0 255.255.0.0
 mac-address 0003.4713.5554
 option 150 ip 10.0.0.1
 default-router 10.0.0.1
!
ip dhcp pool client2
   network 10.0.0.0 255.255.0.0
   mac-address 0030.94C2.9A66
   option 150 ip 10.0.0.1
   default-router 10.0.0.1
!
!
voice lpcor ip-phone subnet incoming
 index 1 local_group1 dhcp-pool client1
 index 2 local_group1 dhcp-pool client2
!
voice lpcor ip-phone subnet outgoing
 index 1 local_group1 dhcp-pool client1
 index 2 local_group1 dhcp-pool client2
!
voice lpcor ip-phone mobility incoming remote_group1
voice lpcor ip-phone mobility outgoing remote_group1
```

The following example shows a LPCOR IP phone subnet configuration with both an IP address network mask and a single shared-address DHCP pool. A specific LPCOR policy can be associated with an IP phone by matching the IP address network mask in the IP-phone subnet table. LPCOR policy local_group2 is associated with the local IP phone with IP address 10.0.10.23. LPCOR local_group2 is associated with the other local IP phones through the DHCP-pool match.

```
ip dhcp pool pool1
   network 10.0.0.0 255.255.0.0
   option 150 ip 10.0.0.1
   default-router 10.0.0.1
!
!
voice lpcor ip-phone subnet incoming
 index 1 local_g2 10.0.10.23 255.255.255.0 vrf vrf-group2
 index 2 remote_g2 172.19.0.0 255.255.0.0
 index 3 local_g1 dhcp-pool pool1
!
voice lpcor ip-phone subnet outgoing
index 1 local_g4 10.1.10.23 255.255.255.0 vrf vrf-group2
index 2 remote_g4 172.19.0.0 255.255.0.0
index 3 local_g5 dhcp-pool pool1
!
voice lpcor ip-phone mobility incoming remote_g1
voice lpcor ip-phone mobility outgoing remote_g1
```

Verify LPCOR Configuration

Use the following **show** commands to display LPCOR configuration information and to verify the LPCOR policy associated with calls.

- **show call active voice—**Displays the LPCOR information for incoming and outgoing call legs (VoIP, ephone, SIP, PSTN).
- **show call history voice—**Displays the LPCOR information for incoming and outgoing call legs (VoIP, ephone, SIP, PSTN). Also displays the LPCOR call-block cause code if the call is blocked due to LPCOR policy validation.
- **show dial-peer voice—**Displays configuration settings for voice dial peers including the LPCOR setting for incoming and outgoing calls.
- **show trunk group—**Displays configuration settings for trunk groups including the LPCOR setting for incoming and outgoing calls.
- **show voice lpcor—**Displays information about LPCOR calls including the LPCOR policy associated with each resource group and directory number, and statistics for failed calls.
- **show voice port—**Displays configuration settings for voice ports including the LPCOR setting for incoming and outgoing calls.

Configuration Examples for LPCOR

Example for Configuring LPCOR for Cisco Unified CME

Figure 43: LPCOR Resource Grouping in Cisco Unified CME Network, on page 1129 shows an example of a Cisco Unified CME network using LPCOR. This network is organized into the following four LPCOR resource groups:

- local_group—Analog and IP phones, including a mobile-type phone, connected locally to Cisco Unified CME.
- pstn_group—Trunks between the PSTN and Cisco Unified CME.
- remote_group—IP phones, including a mobile-type phone, and a SIP proxy server connected remotely to Cisco Unified CME through the WAN.
- voice_mail_group—Cisco Unity Express voice-mail system connected remotely to Cisco Unified CME through the WAN.

Figure 43: LPCOR Resource Grouping in Cisco Unified CME Network

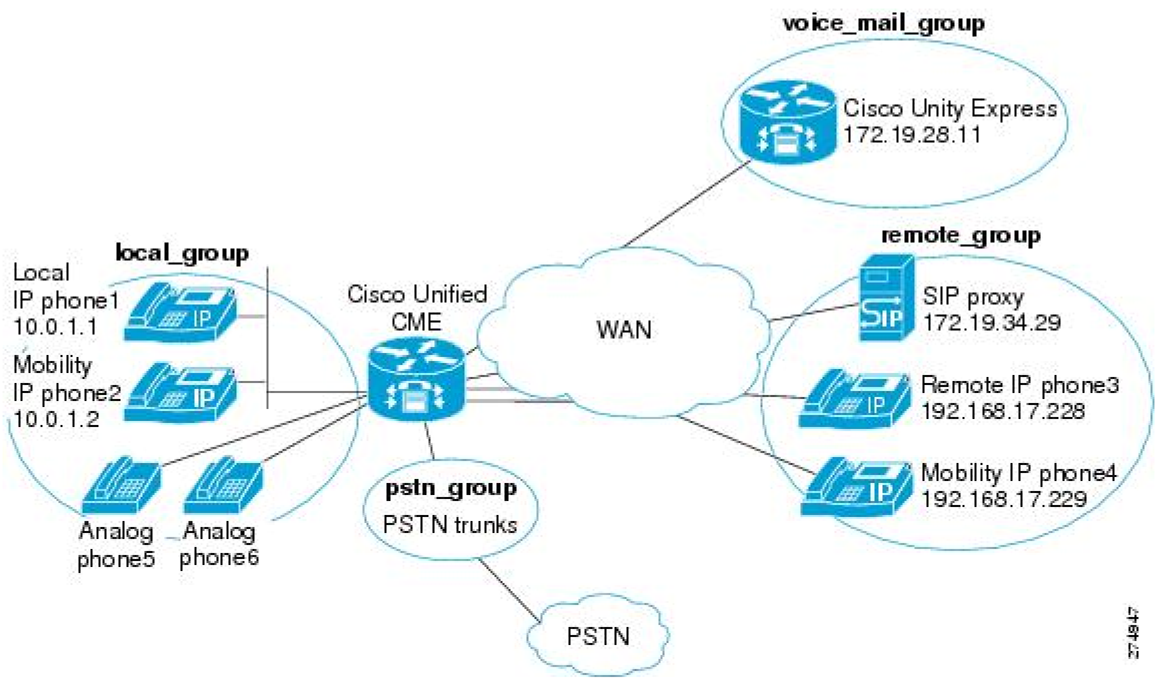
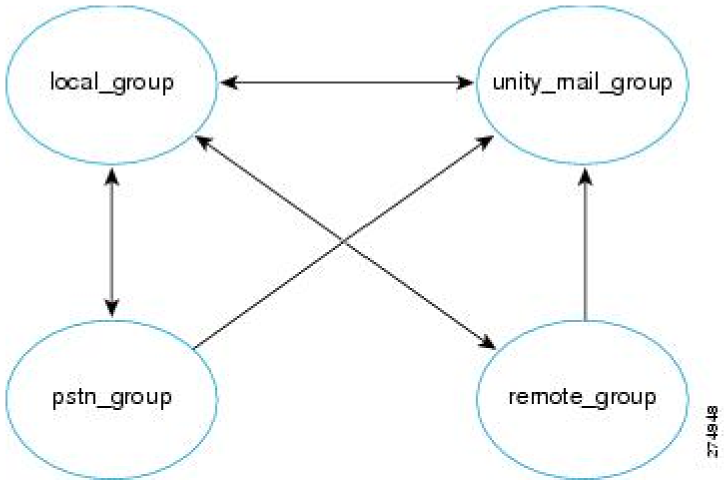


Figure 44: LPCOR Policy Logic, on page 1130 illustrates the access policy between resource groups that provides the following call requirements:

- Blocks calls between remote_group and pstn_group
- Blocks calls from voice_mail_group to pstn_group and remote_group
- Allows calls between local_group and remote_group
- Allows calls between local_group and pstn_group

- Allows all calls to voice_mail_group

Figure 44: LPCOR Policy Logic



The following output shows the LPCOR configuration for this example and describes the steps. Comments describing the configuration are included in the output.

1 Enable LPCOR functionality in Cisco Unified CME and define custom LPCOR group.

```
voice lpcor enable
!
voice lpcor custom
 group 1 pstn_group
 group 2 local_group
 group 3 remote_group
 group 4 voice_mail_group
 !
 #Allow calls only from local group to PSTN group
 voice lpcor policy pstn_group
  accept local_group
 !
 # Allow calls from PSTN, remote, and voice_mail groups to local group
 voice lpcor policy local_group
  accept pstn_group
  accept remote_group
  accept voice_mail_group
 !
 # Allow calls only from local group to remote group
 voice lpcor policy remote_group
  accept local_group
 !
 # Allow calls from PSTN, remote, and local groups to voice_mail group
 voice lpcor voice_mail_group
  accept pstn_group
  accept local_group
  accept remote_group
 !
```

2 Assign LPCOR to the phone, trunk, and IP resources.

```
# analog phone5
voice-port 1/0/0
 lpcor incoming local_group
 lpcor outgoing local_group
!
```

```
# analog phone6
voice-port 1/0/1
 lpcor incoming local_group
 lpcor outgoing local_group
!
# TDM trunks
voice-port 2/1:23
 lpcor incoming pstn_group
 lpcor outgoing pstn_group
!
!
# Specific LPCOR setting for incoming calls from voice_mail_group
voice lpcor ip-trunk subnet incoming
 voice_mail_group 172.19.28.11 255.255.255.255
!
!
# Default LPCOR setting for any incoming VoIP calls
voice service voip
 lpcor incoming remote_group
!
# Cisco Unified CME is DHCP server
ip dhcp pool client1
 network 10.0.0.0 255.255.0.0
 mac-address 0003.4713.5554
  option 150 ip 10.0.0.1
default-router 10.0.0.1
!
# IP phone1 (local)
ephone 1
 lpcor type local
 lpcor incoming local_group
 lpcor outgoing local_group
!
# IP phone2 (mobile)
ephone 2
 lpcor type mobile
!
# IP phone3 (remote)
ephone 3
 lpcor type remote
 lpcor incoming remote_group
 lpcor outgoing remote_group
!
# IP phone4 (mobile)
ephone 4
 lpcor type mobile
!
# IP-phone subnet tables for mobile IP phones
voice lpcor ip-phone subnet incoming
 local_group dhcp-pool pool1
!
voice lpcor ip-phone subnet outgoing
 local_group dhcp-pool client1
!
# Default LPCOR policy for mobile IP phones that
# are not provisioned through IP-phone subnet tables
voice lpcor ip-phone mobility incoming remote_group
voice lpcor ip-phone mobility outgoing remote_group
```

3 Define outgoing LPCOR setting for outgoing VoIP calls.

```
# VoIP outbound dial-peer to Cisco Unity Express mail
dial-peer voice 1234 voip
 destination-pattern 56800
 session target ipv4:172.19.281.1
 pcor outgoing voice_mail_group
!
# VoIP outbound dial-peer to SIP proxy
dial-peer voice 1255 voip
 destination-pattern 1255T
 session protocol sipv2
```

```
    session target sip-server
    lpcor outgoing remote
```

Example for Configuring LPCOR on Cisco 3800 Series Integrated Services Router

```
Router# show running-config

Building configuration...


Current configuration : 10543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
card type t1 2 1
logging message-counter syslog
logging buffered 2000000
no logging console
!
no aaa new-model
network-clock-participate slot 2
!
ip source-route
ip cef
!
!
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.20.1 192.168.20.5
!
ip dhcp pool voice
   network 192.168.20.0 255.255.255.0
   option 150 ip 192.168.20.1
   default-router 192.168.20.1
!
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
!
isdn switch-type primary-5ess
!
voice-card 0
!
voice-card 2
!
!
voice service voip
 notify redirect ip2pots
 allow-connections sip to sip
 sip
  bind control source-interface GigabitEthernet0/1
  bind media source-interface GigabitEthernet0/1
  registrar server expires max 120 min 60
!
!
!
voice class custom-cptone leavetone
 dualtone conference
```

```
  frequency 400 800
  cadence 400 50 200 50 200 50
!
voice class custom-cptone jointone
 dualtone conference
  frequency 600 900
  cadence 300 150 300 100 300 50
!
!
voice iec syslog
voice register global
 mode cme
 source-address 192.168.20.1 port 5060
 max-dn 20
 max-pool 20
 load 7970 SIP70.8-4-2S
 load 7960-7940 P0S3-08-11-00
 authenticate realm cisco.com
 tftp-path flash:
 telnet level 2
 create profile sync 0000312474383825
!
voice register dn  1
 number 4000
 name cme-sip1
 label 4000
!
voice register dn  2
 number 4001
 name cme-sip-2
 label 4001
!
voice register dn  3
 number 4002
 name cme-remote
 label 4002
!
voice register template  1
 softkeys remote-in-use  cBarge Barge Newcall
!
voice register pool  1
 lpcor type local
 lpcor incoming local_sip
 lpcor outgoing local_sip
 id mac 001B.D4C6.AE44
 type 7960
 number 1 dn 1
 dtmf-relay rtp-nte
 codec g711ulaw
!
voice register pool  2
 lpcor type local
 lpcor incoming local_sip
 lpcor outgoing local_sip
 id mac 001E.BE8F.96C1
 type 7940
 number 1 dn 2
 dtmf-relay rtp-nte
 codec g711ulaw
!
voice register pool  3
 lpcor type remote
 lpcor incoming remote_sip
 lpcor outgoing remote_sip
 id mac 001E.BE8F.96C0
 type 7940
 number 1 dn 3
 dtmf-relay rtp-nte
 codec g711ulaw
!
!
voice lpcor enable
voice lpcor call-block cause invalid-number
```

```
voice lpcor custom
 group 1 voip_siptrunk
 group 2 voip_h323trunk
 group 3 pstn_trunk
 group 4 cue_vmail_local
 group 5 cue_vmail_remote
 group 6 vmail_unity
 group 7 local_sccp
 group 8 local_sip
 group 9 remote_sccp
 group 10 remote_sip
 group 11 analog_vg224
 group 12 analog_fxs
 group 13 mobile_phone
!
voice lpcor policy voip_siptrunk
 accept cue_vmail_local
 accept local_sccp
 accept local_sip
 accept analog_vg224
!
voice lpcor policy cue_vmail_local
 accept voip_siptrunk
 accept voip_h323trunk
 accept local_sccp
 accept local_sip
!
voice lpcor policy local_sccp
 accept local_sip
 accept remote_sccp
 accept remote_sip
 accept analog_vg224
 accept analog_fxs
!
voice lpcor policy remote_sccp
 accept local_sccp
 accept local_sip
 accept remote_sip
!
voice lpcor policy analog_vg224
 accept local_sccp
 accept local_sip
 accept remote_sccp
 accept remote_sip
!
voice lpcor policy analog_fxs
 accept local_sccp
 accept local_sip
!
voice lpcor ip-phone subnet incoming
 index 1 local_sccp dhcp-pool voice
!
voice lpcor ip-phone subnet outgoing
 index 1 local_sccp dhcp-pool voice
!
!
!
archive
 log config
  hidekeys
!
!
controller T1 2/0
 cablelength short 133
 pri-group timeslots 1-24
!
controller T1 2/1
!
!
interface Loopback1
 ip address 192.168.21.1 255.255.255.0
 ip ospf network point-to-point
!
```

```
interface GigabitEthernet0/0
 ip address 192.168.160.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface FastEthernet0/2/0
 ip address 192.168.98.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/2/1
 no ip address
 duplex auto
 speed auto
!
interface Service-Engine1/0
 ip unnumbered Loopback1
 service-module ip address 192.168.21.100 255.255.255.0
 service-module ip default-gateway 192.168.21.1
!
interface Serial2/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 no cdp enable
!
router ospf 1
 log-adjacency-changes
 network 192.168.160.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.21.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 192.168.21.100 255.255.255.255 Service-Engine1/0
!
!
no ip http server
!
!
tftp-server flash:term41.default.loads
tftp-server flash:term61.default.loads
tftp-server flash:SCCP41.8-3-1S.loads
tftp-server flash:apps41.8-3-0-50.sbn
tftp-server flash:cnu41.8-3-0-50.sbn
tftp-server flash:P003-08-11-00.bin
tftp-server flash:P003-08-11-00.sbn
tftp-server flash:P0S3-08-11-00.sb2
tftp-server flash:P0S3-08-11-00.loads
tftp-server flash:term71.default.loads
tftp-server flash:term70.default.loads
tftp-server flash:jar70sccp.8-2-2TR2.sbn
tftp-server flash:dsp70.8-2-2TR2.sbn
tftp-server flash:cvm70sccp.8-2-2TR2.sbn
tftp-server flash:apps70.8-2-2TR2.sbn
tftp-server flash:SCCP70.8-2-2SR2S.loads
!
control-plane
!
!
voice-port 0/1/0
 lpcor incoming analog_fxs
 lpcor outgoing analog_fxs
 station-id name FXS-Phone
 station-id number 3000
 caller-id enable
```

```
!
voice-port 0/1/1
!
voice-port 2/0:23
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
!
dial-peer voice 2 voip
 destination-pattern 2...
 lpcor outgoing voip_siptrunk
 session protocol sipv2
 session target ipv4:192.168.97.1
 codec g711ulaw
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
!
dial-peer voice 5050 voip
 description *** VMAIL Dial-Peer ***
 destination-pattern 5...
 lpcor outgoing cue_vmail_local
 session protocol sipv2
 session target ipv4:192.168.21.100
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 30 pots
 destination-pattern 3000
 direct-inward-dial
 port 0/1/0
!
!
sip-ua
 mwi-server ipv4:192.168.21.100 expires 3600 port 5060 transport udp
 registrar ipv4:192.168.21.1 expires 3600
!
!
telephony-service
 em logout 0:0 0:0 0:0
 max-ephones 15
 max-dn 15
 ip source-address 192.168.20.1 port 2000
 service phone videoCapability 1
 load 7941 SCCP41.8-3-1S
 date-format dd-mm-yy
 voicemail 5050
 max-conferences 12 gain -6
 transfer-system full-consult
 transfer-pattern .T
 transfer-pattern ....
 fac standard
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-template  1
 softkeys hold  Join Newcall Resume Select
 softkeys idle  Cfwdall ConfList Dnd Join Newcall Pickup Redial RmLstC
 softkeys seized  Endcall Redial Cfwdall Pickup
!
!
ephone-template  2
 lpcor type remote
 lpcor incoming remote_sccp
 lpcor outgoing remote_sccp
!
!
ephone-dn  1  dual-line
 number 5000
 call-forward busy 5050
```

```
 call-forward noan 5050 timeout 10
 mwi sip
!
!
ephone-dn  2  dual-line
 number 5001
 call-forward busy 5050
 call-forward noan 5050 timeout 10
 mwi sip
!
!
ephone-dn  3  dual-line
 number 5010
 description vg224-1/1
 name analog-1
!
!
ephone-dn  4  dual-line
 number 5011
 description vg224-1/2
 name analog-2
!
!
ephone-dn  5  dual-line
 number 5012
 description vg224-1/3
 name analog-3
!
!
ephone-dn  6  dual-line
 number 5013
 description vg224-1/4
 name analog-4
!
!
ephone-dn  7  dual-line
 number 5020
 name SCCP-Remote
 mwi sip
!
!
ephone  1
 lpcor type local
 lpcor incoming local_sccp
 lpcor outgoing local_sccp
 mac-address 001E.7A26.EB60
 ephone-template 1
 type 7941
 button  1:1
!
!
!
ephone  2
 lpcor type local
 lpcor incoming local_sccp
 lpcor outgoing local_sccp
 mac-address 001E.7AC2.CCF9
 ephone-template 1
 type 7941
 button  1:2
!
!
!
ephone  3
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2400
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:3
!
```

```
!
!
ephone  4
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2401
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:4
!
!
!
ephone  5
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2402
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:5
!
!
!
ephone  6
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2403
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:6
!
!
!
ephone  7
 mac-address 001B.D52C.DF1F
 ephone-template 2
 type 7970
 button  1:7
!
!
alias exec cue ser ser 1/0 sess
!
line con 0
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
endRouter# show running-config

Building configuration...


Current configuration : 10543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
```

```
!
boot-start-marker
boot-end-marker
!
card type t1 2 1
logging message-counter syslog
logging buffered 2000000
no logging console
!
no aaa new-model
network-clock-participate slot 2
!
ip source-route
ip cef
!
!
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.20.1 192.168.20.5
!
ip dhcp pool voice
   network 192.168.20.0 255.255.255.0
   option 150 ip 192.168.20.1
   default-router 192.168.20.1
!
!
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
!
!
isdn switch-type primary-5ess
!
voice-card 0
!
voice-card 2
!
!
voice service voip
 notify redirect ip2pots
 allow-connections sip to sip
 sip
  bind control source-interface GigabitEthernet0/1
  bind media source-interface GigabitEthernet0/1
  registrar server expires max 120 min 60
!
!
!
voice class custom-cptone leavetone
 dualtone conference
  frequency 400 800
  cadence 400 50 200 50 200 50
!
voice class custom-cptone jointone
 dualtone conference
  frequency 600 900
  cadence 300 150 300 100 300 50
!
!
voice iec syslog
voice register global
 mode cme
 source-address 192.168.20.1 port 5060
 max-dn 20
 max-pool 20
 load 7970 SIP70.8-4-2S
 load 7960-7940 P0S3-08-11-00
 authenticate realm cisco.com
 tftp-path flash:
 telnet level 2
 create profile sync 0000312474383825
!
voice register dn  1
 number 4000
```

```
 name cme-sip1
 label 4000
!
voice register dn  2
 number 4001
 name cme-sip-2
 label 4001
!
voice register dn  3
 number 4002
 name cme-remote
 label 4002
!
voice register template  1
 softkeys remote-in-use  cBarge Barge Newcall
!
voice register pool  1
 lpcor type local
 lpcor incoming local_sip
 lpcor outgoing local_sip
 id mac 001B.D4C6.AE44
 type 7960
 number 1 dn 1
 dtmf-relay rtp-nte
 codec g711ulaw
!
voice register pool  2
 lpcor type local
 lpcor incoming local_sip
 lpcor outgoing local_sip
 id mac 001E.BE8F.96C1
 type 7940
 number 1 dn 2
 dtmf-relay rtp-nte
 codec g711ulaw
!
voice register pool  3
 lpcor type remote
 lpcor incoming remote_sip
 lpcor outgoing remote_sip
 id mac 001E.BE8F.96C0
 type 7940
 number 1 dn 3
 dtmf-relay rtp-nte
 codec g711ulaw
!
!
voice lpcor enable
voice lpcor call-block cause invalid-number
voice lpcor custom
 group 1 voip_siptrunk
 group 2 voip_h323trunk
 group 3 pstn_trunk
 group 4 cue_vmail_local
 group 5 cue_vmail_remote
 group 6 vmail_unity
 group 7 local_sccp
 group 8 local_sip
 group 9 remote_sccp
 group 10 remote_sip
 group 11 analog_vg224
 group 12 analog_fxs
 group 13 mobile_phone
!
voice lpcor policy voip_siptrunk
 accept cue_vmail_local
 accept local_sccp
 accept local_sip
 accept analog_vg224
!
voice lpcor policy cue_vmail_local
 accept voip_siptrunk
 accept voip_h323trunk
```

```
 accept local_sccp
 accept local_sip
!
voice lpcor policy local_sccp
 accept local_sip
 accept remote_sccp
 accept remote_sip
 accept analog_vg224
 accept analog_fxs
!
voice lpcor policy remote_sccp
 accept local_sccp
 accept local_sip
 accept remote_sip
!
voice lpcor policy analog_vg224
 accept local_sccp
 accept local_sip
 accept remote_sccp
 accept remote_sip
!
voice lpcor policy analog_fxs
 accept local_sccp
 accept local_sip
!
voice lpcor ip-phone subnet incoming
 index 1 local_sccp dhcp-pool voice
!
voice lpcor ip-phone subnet outgoing
 index 1 local_sccp dhcp-pool voice
!
!
!
archive
 log config
  hidekeys
!
!
controller T1 2/0
 cablelength short 133
 pri-group timeslots 1-24
!
controller T1 2/1
!
!
interface Loopback1
 ip address 192.168.21.1 255.255.255.0
 ip ospf network point-to-point
!
interface GigabitEthernet0/0
 ip address 192.168.160.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface FastEthernet0/2/0
 ip address 192.168.98.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/2/1
 no ip address
 duplex auto
 speed auto
!
interface Service-Engine1/0
 ip unnumbered Loopback1
```

```
 service-module ip address 192.168.21.100 255.255.255.0
 service-module ip default-gateway 192.168.21.1
!
interface Serial2/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 no cdp enable
!
router ospf 1
 log-adjacency-changes
 network 192.168.160.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.21.0 0.0.0.255 area 0
!
ip forward-protocol nd
ip route 192.168.21.100 255.255.255.255 Service-Engine1/0
!
!
no ip http server
!
!
tftp-server flash:term41.default.loads
tftp-server flash:term61.default.loads
tftp-server flash:SCCP41.8-3-1S.loads
tftp-server flash:apps41.8-3-0-50.sbn
tftp-server flash:cnu41.8-3-0-50.sbn
tftp-server flash:P003-08-11-00.bin
tftp-server flash:P003-08-11-00.sbn
tftp-server flash:P0S3-08-11-00.sb2
tftp-server flash:P0S3-08-11-00.loads
tftp-server flash:term71.default.loads
tftp-server flash:term70.default.loads
tftp-server flash:jar70sccp.8-2-2TR2.sbn
tftp-server flash:dsp70.8-2-2TR2.sbn
tftp-server flash:cvm70sccp.8-2-2TR2.sbn
tftp-server flash:apps70.8-2-2TR2.sbn
tftp-server flash:SCCP70.8-2-2SR2S.loads
!
control-plane
!
!
voice-port 0/1/0
 lpcor incoming analog_fxs
 lpcor outgoing analog_fxs
 station-id name FXS-Phone
 station-id number 3000
 caller-id enable
!
voice-port 0/1/1
!
voice-port 2/0:23
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
!
dial-peer voice 2 voip
 destination-pattern 2...
 lpcor outgoing voip_siptrunk
 session protocol sipv2
 session target ipv4:192.168.97.1
 codec g711ulaw
 ip qos dscp cs5 media
 ip qos dscp cs4 signaling
!
dial-peer voice 5050 voip
 description *** VMAIL Dial-Peer ***
 destination-pattern 5...
 lpcor outgoing cue_vmail_local
```

```
 session protocol sipv2
 session target ipv4:192.168.21.100
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 30 pots
 destination-pattern 3000
 direct-inward-dial
 port 0/1/0
!
!
sip-ua
 mwi-server ipv4:192.168.21.100 expires 3600 port 5060 transport udp
 registrar ipv4:192.168.21.1 expires 3600
!
!
telephony-service
 em logout 0:0 0:0 0:0
 max-ephones 15
 max-dn 15
 ip source-address 192.168.20.1 port 2000
 service phone videoCapability 1
 load 7941 SCCP41.8-3-1S
 date-format dd-mm-yy
 voicemail 5050
 max-conferences 12 gain -6
 transfer-system full-consult
 transfer-pattern .T
 transfer-pattern ....
 fac standard
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-template  1
 softkeys hold  Join Newcall Resume Select
 softkeys idle  Cfwdall ConfList Dnd Join Newcall Pickup Redial RmLstC
 softkeys seized  Endcall Redial Cfwdall Pickup
!
!
ephone-template  2
 lpcor type remote
 lpcor incoming remote_sccp
 lpcor outgoing remote_sccp
!
!
ephone-dn  1  dual-line
 number 5000
 call-forward busy 5050
 call-forward noan 5050 timeout 10
 mwi sip
!
!
ephone-dn  2  dual-line
 number 5001
 call-forward busy 5050
 call-forward noan 5050 timeout 10
 mwi sip
!
!
ephone-dn  3  dual-line
 number 5010
 description vg224-1/1
 name analog-1
!
!
ephone-dn  4  dual-line
 number 5011
 description vg224-1/2
 name analog-2
!
!
ephone-dn  5  dual-line
```

```
 number 5012
 description vg224-1/3
 name analog-3
!
!
ephone-dn  6  dual-line
 number 5013
 description vg224-1/4
 name analog-4
!
!
ephone-dn  7  dual-line
 number 5020
 name SCCP-Remote
 mwi sip
!
!
ephone  1
 lpcor type local
 lpcor incoming local_sccp
 lpcor outgoing local_sccp
 mac-address 001E.7A26.EB60
 ephone-template 1
 type 7941
 button  1:1
!
!
!
ephone  2
 lpcor type local
 lpcor incoming local_sccp
 lpcor outgoing local_sccp
 mac-address 001E.7AC2.CCF9
 ephone-template 1
 type 7941
 button  1:2
!
!
!
ephone  3
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2400
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:3
!
!
!
ephone  4
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2401
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:4
!
!
!
ephone  5
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2402
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:5
!
```

```
!
!
ephone  6
 lpcor type local
 lpcor incoming analog_vg224
 lpcor outgoing analog_vg224
 mac-address F9E5.8B28.2403
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:6
!
!
!
ephone  7
 mac-address 001B.D52C.DF1F
 ephone-template 2
 type 7970
 button  1:7
!
!
alias exec cue ser ser 1/0 sess
!
line con 0
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Feature Information for LPCOR

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

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

Table 97: Feature Information for LPCOR

Feature Name	Cisco Unified CME Version	Feature Information
Call Restriction Regulations for Cisco Unified CME	8.0	Introduced support for LPCOR feature.

CHAPTER 43

Call Transfer and Forward

Information About Call Transfer and Forward

Call Forward

Call forward feature diverts calls to a specified number under one or more of the following conditions:

- All calls—When all-call call forwarding is activated by a phone user, all incoming calls are diverted. The target destination for diverted calls can be specified in the router configuration or by the phone user with a soft key or feature access code. The most recently entered destination is recognized by Cisco Unified CME, regardless of how it was entered.
- No answer—Incoming calls are diverted when the extension does not answer before the timeout expires. The target destination for diverted calls is specified in the router configuration.
- Busy—Incoming calls are diverted when the extension is busy and call waiting is not active. The target destination for diverted calls is specified in the router configuration.
- Night service—All incoming calls are automatically diverted during night-service hours. The target destination for diverted calls is specified in the router configuration.

A directory number can have all four types of call forwarding defined at the same time with a different forwarding destination defined for each type of call forwarding. If more than one type of call forwarding is active at one time, the order for evaluating the different types is as follows:

1. Call forward night-service
2. Call forward all

3 Call forward busy and call forward no-answer

H.450.3 capabilities are enabled globally on the router by default, and can be disabled either globally or for individual dial peers. You can configure incoming patterns for using the H.450.3 standard. Calling-party numbers that do not match the patterns defined with this command are forwarded using Cisco-proprietary call forwarding for backward compatibility. For information about configuring H.450.3 on a Cisco Unified CME system, see Enable Call Forwarding for a Directory Number, on page 1185.

Selective Call Forward

You can apply call forward to a busy or no-answer directory number based on the number that is dialed to reach the directory number: the primary number, the secondary number, or either of those numbers expanded by a dial-plan pattern.

Cisco Unified CME automatically creates one POTS dial peer for each ephone-dn when it is assigned a primary number. If the ephone-dn is assigned a secondary number, it creates a second POTS dial peer. If the **dialplan-pattern** command is used to expand the primary and secondary numbers for ephone-dns, it creates two more dial peers, resulting in the creation of the following four dial peers for the ephone-dn:

- A POTS dial peer for the primary number
- A POTS dial peer for the secondary number
- A POTS dial peer for the primary number as expanded by the **dialplan-pattern** command
- A POTS dial peer for the secondary number as expanded by the **dialplan-pattern** command

Call forwarding is normally applied to all dial peers created for an ephone-dn. Selective call forwarding allows you to apply call forwarding for busy or no-answer calls only for the dial peers you have specified, based on the called number that was used to route the call to the ephone-dn.

```
For example, the following commands set up a single ephone-dn (ephone-dn 5) with four dial
 peers:
telephony-service
 dialplan-pattern 1 40855501.. extension-length 4 extension-pattern 50..

ephone-dn 5
 number 5066 secondary 5067
```

In this example, selective call forwarding can be applied so that calls are forwarded when:

- callers dial the primary number 5066.
- when callers dial the secondary number 5067.
- when callers dial the expanded numbers 4085550166 or 4085550167.

For configuration information, see Enable Call Forwarding for a Directory Number, on page 1185.

Call Forward Unregistered

The Call Forward Unregistered (CFU) feature allows you to forward a call to a different number if the directory number (DN) is not associated with a phone or if the associated phone is not registered to Cisco Unified CME. The CFU feature is very useful for wireless phone users when the wireless phone is out of the access point or phone shuts down automatically because of an automatic shutdown feature. The service is not available and the call can be forwarded to the CFU destination. Any unregistered or floating DN can be forwarded using the CFU feature.

An unregistered DN indicates that none of its associated phones are registered to the Cisco Unified CME. A registered phone will become unregistered when the Cisco Unified CME sends an unregistration request or responses to a phone's unregistration request. Cisco Unified CME sends an unregistration request under the following circumstances:

- When the keepalive timer expires.
- When a user issues a reset or restart command on the phone.
- When an extension mobility (EM) user logs into the phone. (All DNs configured under the logout-profile are unregistered except for the shared ones that are associated with other registered phones.)
- When an EM user logs out of the phone. (All DNs configured under the user-profile are unregistered except for the shared ones that are associated with other registered phones.)

There is always a gap between the time the phone loses its connection with Cisco Unified CME and the time when Cisco Unified CME claims the phone is unregistered. The length of the gap depends on the keepalive timer. Cisco Unified CME considers the phone as registered and tries to associate DNs until the keepalive timer expires. You can configure the expiration for the keepalive timer using the registrar server expires max <seconds> min <seconds> command under sip in voice service voip mode for SIP IP phones. For more information, see Example for Configuring Keepalive Timer Expiration in SIP Phones, on page 1232.

Cisco Unified CME 8.6 supports the CFU feature on SIP IP phones using the call-forward b2bua unregistered command under voice register dn tag. The CFU feature supports overlap dialing and en-bloc dialing. A call to a floating DN is forwarded to its CFU destination, if configured. Calls to a DN out of service point or phones losing connection are not forwarded to a CFU number until the phone becomes unregistered. For more information on configuring call-forward unregistered, see Example for Configuring Call Forward Unregistered for SIP IP Phones, on page 1232.

Note In earlier versions of Cisco Unified CME, a busy tone was played for callers when the callers are unable to reach the SCCP phone number. In Cisco Unified CME 8.6 and later versions, a fast busy tone is played instead of a busy tone for callers who are unable to reach the phone.

B2BUA Call Forward for SIP Devices

Cisco Unified CME 3.4 an d later versions acts as both UA server and UA client; that is, as a B2BUA. Calls into a SIP phone can be forwarded to other SIP or SCCP devices (including Cisco Unity or Cisco Unity Express, third-party voice mail systems, an auto attendant or an IVR system, such as Cisco Unified IPCC and Cisco Unified IPCC Express). In addition, SCCP phones can be forwarded to SIP phones.

Cisco Unity or other voice-messaging systems connected by a SIP trunk or SIP user agent are able to pass an MWI to a SIP phone when a call is forwarded. The SIP phone then displays the MWI when indicated by the voice-messaging system.

The call-forward busy response is triggered when a call is sent to a SIP phone using a VoIP dial peer and a busy response is received back from the phone. SIP-to-SIP call forwarding is invoked only if the phone is dialed directly. Call forwarding is not invoked when the phone number is called through a sequential, longest-idle, or peer hunt group.

You can configure call forwarding for an individual directory number, or for every number on a SIP phone. If the information is configured in both, the information under voice register dn takes precedence over the information configured under voice register pool.

For configuration information, see Configure SIP-to-SIP Phone Call Forwarding, on page 1213.

Call Forward All Synchronization for SIP Phones

The Call Forward All feature allows users to forward all incoming calls to a phone number that they specify. This feature is supported on all SIP phones and can be provisioned from either Cisco Unified CME or the individual SIP phone. Before Cisco Unified CME 4.1, there was no method for exchanging the Call Forward All configuration between Cisco Unified CME and the SIP phone. If Call Forward All was enabled on the phone, the configuration in Cisco Unified CME was not updated; conversely, the configuration in Cisco Unified CME was not sent to the phone.

In Cisco Unified CME 4.1 and later, the following enhancements are supported for the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE to keep the configuration consistent between Cisco Unified CME and the SIP phone:

- When Call Forward All is configured on Cisco Unified CME with the **call-forward b2bua all** command, the configuration is sent to the phone which updates the CfwdAll soft key to indicate that Call forward All is enabled. Because Call Forward All is configured on a per line basis, the CfwdAll soft key is updated only when Call Forward All is enabled for the primary line.
- When a user enables Call Forward All on a phone using the CfwdAll soft key, the uniform resource identifier (URI) for the service (defined with the **call-feature-uri** command) and the call forward number (unless Call Forward All is disabled) is sent to Cisco Unified CME. It updates its voice register pool and voice register dn configuration with the **call-forward b2bua all** command to be consistent with the phone configuration.
- Call Forward All supports KPML so that a user does not need to press the Dial or # key, or wait for the interdigit timeout, to configure the Call Forward All number. Cisco Unified CME collects the Call Forward All digits until it finds a match in the dial peers.

For configuration information, see Configure Call-Forwarding-All Softkey URI on SIP Phones, on page 1218.

Call Transfer

When you are connected to another party, call transfer allows you to shift the connection of the other party to a different number. Call transfer methods must inter-operate with systems in the other networks with which you interface. Cisco CME 3.2 and later versions provide full call-transfer and call-forwarding interoperability with call processing systems that support H.450.2, H.450.3, and H.450.12 standards. For call processing systems that do not support H.450 standards, Cisco CME 3.2 and later versions provide VoIP-to-VoIP hairpin call routing.

Call transfers can be blind or consultative. A blind transfer is one in which the transferring extension connects the caller to a destination extension before ringback begins. A consultative transfer is one in which the transferring 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.

You can configure blind or consultative transfer on a system-wide basis or for individual extensions. For example, in a system that is set up for consultative transfer, a specific extension with an auto-attendant that automatically transfers incoming calls to specific extension numbers can be set to use blind transfer, because auto-attendants do not use consultative transfer.

Call Transfer Blocking

Transfers to all numbers except those on local phones are automatically blocked by default. During configuration, you can allow transfers to nonlocal numbers. In Cisco Unified CME 4.0 and later versions, you can prevent individual phones from transferring calls to numbers that are globally enabled for transfer. This ensures that individual phones do not incur toll charges by transferring calls outside the Cisco Unified CME system. Call transfer blocking can be configured for individual phones or configured as part of a template that is applied to a set of phones.

Another way to eliminate toll charges on call transfers is to limit the number of digits that phone users can dial when transferring calls. For example, if you specify a maximum of eight digits in the configuration, users who are transferring calls can dial one digit for external access and seven digits more, which is generally enough for a local number but not a long-distance number. In most locations, this plan will limit transfers to nontoll destinations. Long-distance calls, which typically require ten digits or more, will not be allowed. This configuration is only necessary when global transfer to numbers outside the Cisco Unified CME system has been enabled using the **transfer-pattern** (telephony-service) command. Transfers to numbers outside the Cisco Unified CME system are not permitted by default.

For configuration information, see Configure Call Transfer Options for SCCP Phones, on page 1189.

Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones

In Cisco Unified CME 4.0 trunk-to-trunk transfer blocking for toll bypass fraud prevention is supported on Cisco Unified Skinny Client Control Protocol (SCCP) IP phones.

In Cisco Unified CME 9.5, trunk-to-trunk transfer blocking for toll bypass fraud prevention is also supported on Cisco Unified Session Initiation Protocol (SIP) IP phones.

In Cisco Unified CME 10.5, trunk-to-trunk conference blocking is also supported on Cisco Unified Skinny Client Control Protocol (SCCP) and Cisco Unified Session Initiation Protocol (SIP) IP phones.

Table 98: Configuration Modes for Transfer-Blocking Commands, on page 1151 lists the transfer-blocking commands and the appropriate configuration modes for Cisco Unified CME and Cisco Unified SRST.

Table 98: Configuration Modes for Transfer-Blocking Commands

Commands	Cisco Unified CME
transfer-pattern	telephony-service
transfer max-length	voice register pool or voice register template
transfer-pattern blocked	voice register pool or voice register template
conference transfer-pattern	telephony-service

Commands	Cisco Unified CME
conference max-length	ephone ephone-template voice register pool voice register template
conference-pattern blocked	ephone ephone-template voice register pool voice register template

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

Transfer Pattern

The **transfer-pattern** command for Cisco Unified SCCP IP phones is extended to Cisco Unified SIP IP phones.

The **transfer-pattern** command specifies the directory numbers for call transfer. The command can be configured up to 32 times using the following command syntax:
transfer-pattern *transfer-pattern* `[blind]`

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

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

Note In Cisco Unified CME 9.5 and later versions, Cisco Unified SIP IP phones and Cisco Unified SCCP IP phones registered to the same Cisco Unified CME are considered local and do not require transfer-pattern configuration.

The following are examples of configurable transfer patterns:

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

Backward Compatibility

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

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

Dial Plans

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

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

Note In Cisco Unified CME 9.5 and later versions, once transfer patterns are configured in telephony-service configuration mode, the transfer patterns apply to both Cisco Unified SCCP IP phones and Cisco Unified SIP IP phones.

Transfer Max-Length

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

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

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

Conference Max-Length

Conference calls are allowed when:

- both **conference transfer-pattern** and **transfer-pattern** commands are configured
- dialed digits match the configured transfer pattern

When conference max-length command is configured, the Cisco Unified CME will allow the conferences only if the dialed digits are within the max-length limit.

If configured, the conference max-length command does not impact call transfers.

Note If both **conference max-length** and **transfer max-length** commands are configured, the conference **max-length** command takes precedence for conferences.

Conference-Pattern Blocked

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

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

	conference max-length	no conference max-length
No conference-pattern blocked (default case)	Allowing/Blocking of conference call depends on configured conference max-length	Allowing/Blocking of conference call depends on configured transfer max-length
conference-pattern blocked	No conference calls allowed for SIP and SCCP phones.	

	Max-length <= allowed max-length		**Max-length > allowed max-length**	
	Transfer	Conference	Transfer	Conference
Transfer max-length + No Conference max-length (use transfer max-length for conference cases too, as conference max-length not configured)	Y	Y	N	N
No transfer max-length + Conference max-length (conference max-length has precedence over transfer max-length for conference)	Y	Y	Y	N

No transfer max-length + Conference max-length (conference max-length has precedence over transfer max-length for conference)	Y	Y	N	N
No transfer max-length + No conference max-length	All transfer and conference calls are allowed.			

Configure the Maximum Number of Digits for a Conference Call

Before You Begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
    - **voice register pool** *pool-tag*
    - **voice register template** *template-tag*
    - **ephone** *phone-tag*
    - **ephone template** *template-tag*
4. **conference max-length** value
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **voice register pool** *pool-tag* • **voice register template** *template-tag* • **ephone** *phone-tag* • **ephone template** *template-tag* **Example:** `Router(config)# voice register pool 25`	Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME. • *pool-tag*—Unique number assigned to the pool. Range is 1 to 100. or Enters voice register template configuration mode and defines a template of common parameters for Cisco Unified SIP IP phones. • *template-tag*—Declares a template tag. Range is 1 to 10. or Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type? to display range.
Step 4	**conference max-length** value **Example:** `Router(config-register-pool)# conference max-length 6`	Allows the conference calls from Cisco IP phones to specified directory numbers of phones. • conference max-length—Specifies the maximum number of digits while making a conference call. Range is 3 to 16.
Step 5	**exit** **Example:** `Router(config-register-pool)# exit`	Exits voice register pool configuration mode and enters global configuration mode.

Configure Conference Blocking Options for Phones

To prevent extensions from making conference calls to directory numbers that are otherwise allowed globally.

Before You Begin

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **voice register pool** *pool-tag* or
   - **voice register template** *template-tag*
   - **ephone** *phone-tag*
   - **ephone template** *template-tag*
4. **conference-pattern blocked**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **voice register pool** *pool-tag* or • **voice register template** *template-tag* • **ephone** *phone-tag* • **ephone template** *template-tag* **Example:** `Router(config)# voice register pool 25`	Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME or for a set of Cisco Unified SIP IP phones in Cisco Unified SIP SRST. • pool-tag—Unique number assigned to the pool. Range is 1 to 100. or Enters voice register template configuration mode and defines a template of common parameters for Cisco Unified SIP IP phones. • template-tag—Declares a template tag. Range is 1 to 10. or Enters ephone configuration mode. • phone-tag—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type? to display range.
Step 4	**conference-pattern blocked**	Blocks conference calls to external numbers.

	Command or Action	Purpose
	Example: `Router(config-register-pool)#`	• conference-pattern block—Prevents extensions on an ephone or a voice register pool from initiating conferences.
Step 5	**exit** **Example:** `Router(config-register-pool)# exit`	Exits voice register pool configuration mode.

Transfer-Pattern Blocked

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

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

Table 99: Behaviors of Cisco Unified IP Phones for Specific Configurations, on page 1158 compares the behaviors of Cisco Unified SCCP and SIP IP phones for specific configurations.

Table 99: Behaviors of Cisco Unified IP Phones for Specific Configurations

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

Conference Transfer-Pattern

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

For configuration information, see Specify Transfer Patterns for Trunk-to-Trunk Calls and Conferences for SIP, on page 1192 and Conference-Pattern Blocked, on page 1154 and Conference Max-Length, on page 1153.

For configuration examples, see Example for Configuring Conference Transfer Patterns, on page 1224, Example for Configuring Maximum Length of Transfer Number, on page 1224, Example for Configuring Transfer Patterns, on page 1224, and Example for Blocking All Call Transfers, on page 1224.

Call Transfer Recall on SCCP Phones

The Call Transfer Recall feature in Cisco Unified CME 4.3 and later versions returns a transferred call to the phone that initiated the transfer if the destination is busy or does not answer. After a phone user completes a transfer to a directory number on a local phone, if the transfer-to party does not answer before the configured recall timer expires, the call is directed back to the transferor phone. The message “Transfer Recall From *xxxx*” displays on the transferor phone.

The transfer-to directory number cannot have Call Forward Busy enabled, or it cannot be a hunt group pilot number. If the transfer-to directory number has Call Forward No Answer (CFNA) enabled, Cisco Unified CME recalls the call only if the transfer-recall timeout is set to less than the CFNA timeout. If the transfer-recall timeout is set to more than the CFNA timeout, the call is forwarded to the CFNA target number after the transfer-to party does not answer.

If the transferor phone is busy, Cisco Unified CME attempts the recall again after the transfer-recall timeout value expires. Cisco Unified CME attempts a recall up to three times. If the transferor phone remains busy, the call is disconnected after the third recall attempt.

The transferor phone and transfer-to phone must be registered to the same Cisco Unified CME, however the transferee phone can be remote.

For configuration information, see Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.

Call Transfer Recall on SIP Phones

From Unified CME 11.6 onwards, Call Transfer Recall feature is supported on SIP phones. This feature returns a transferred call to the phone that initiated the transfer if the destination is busy or does not answer. After a phone user completes a transfer to a directory number on a local SIP phone, and if the transfer-to party does not answer before the configured recall timer expires, the call is directed back to the transferor phone. The message "Transfer Recall From *xxxx* " displays on the transferor phone.

The Call Transfer Recall in SIP phones is achieved using the CLI **timeouts transfer-recall** command in voice register dn or voice register global configuration modes.

The transfer-to directory number cannot have Call Forward Busy enabled, or it cannot be a hunt group pilot number. The transferor phone and transfer-to phone must be registered to the same Cisco Unified CME, however the transferee phone can be remote. If the transfer-to directory number has Call Forward No Answer (CFNA) enabled, Cisco Unified CME recalls the call only if the transfer-recall timeout is set to less than the CFNA timeout. If the transfer-recall timeout is set to more than the CFNA timeout, the call is forwarded to the CFNA target number after the transfer-to party does not answer. If the transfer-recall timeout is equal to the CFNA timeout, the call is forwarded to the CFNA target number as the CFNA timeout expires before the transfer-recall timeout.

When Call Forward All is configured in Cisco Unified CME, the call is forwarded directly to call forward target number irrespective of whether the phone is busy or idle. In this scenario, transfer recall is not applicable after the call is forwarded.

If the transferor phone is busy, Cisco Unified CME attempts the recall again after the transfer-recall timeout value expires. Cisco Unified CME attempts a recall up to three times. If the transferor phone remains busy, the call is disconnected after the third recall attempt. Also, if the transferor phone is a shared line, and if one of the phones is idle, the transfer recall is directed to the transferor phone that is idle.

When Single Number Reach (SNR) is configured in Cisco Unified CME, the desk IP Phone rings first. If the desk IP Phone does not answer within the configured SNR timer expiry value, the configured remote number (mobile) starts ringing while continuing to ring the desk IP Phone. If both the extensions does not answer the call, transfer recall is directed back to the transferor phone. Transfer recall does not happen if the desk IP Phone or remote phone (mobile) is busy. Also, transfer recall does not happen if one of the SNR extensions answers the call.

For configuration information, see Enable Call-Transfer Recall on SIP Phones at System-Level, on page 1183.

From Cisco Unified CME release 11.6 onwards, call transfer recall feature supports mixed deployment of SCCP and SIP phones. In a mixed deployment scenario, you can have a SIP phone as transferor and with an SCCP phone being transfer-to or vice versa.

In mixed mode, if the transfer recall is performed with multiple SIP or SCCP transferors and a single transfer-to SCCP phone, transfer recall display messages are displayed on both the transferors. Here, transfer recall happens for all the calls when the destination is busy or does not answer the call. In the case of single transfer-to SIP phones, only the first phone call is recalled even if dual-line is configured.

Consultative-Transfer Enhancements in Cisco Unified CME 4.3 and Later Versions

Cisco Unified CME 4.3 modifies the digit-collection process for consultative call transfers. After a phone user presses the Transfer soft key to make a consultative transfer, a new consultative call leg is created and the Transfer soft key is not displayed again until the dialed digits of the transfer-to number are matched to a transfer pattern and the consultative call leg is in the alerting state.

Transfer-to digits dialed by the phone user are no longer buffered. The dialed digits, except the call park FAC code, are collected on the seized consultative call-leg until the digits match a pattern for consultative transfer, blind transfer, park-slot transfer, park-slot transfer blocking, or PSTN transfer blocking. The existing pattern matching process is unchanged, and you have the option of using this new transfer digit-collection method or reverting to the former method.

Before Cisco Unified CME 4.3, the consultative transfer feature collects dialed digits on the original call leg until the digits either match a transfer pattern or blocking pattern. When the transfer-to number is matched, and PSTN blocking is not enabled, the original call is put on hold and an idle line or channel is seized to send the dialed digits from the buffer.

The method of matching a pattern for consultative transfer, blind transfer, park-slot transfer, park-slot transfer blocking, PSTN transfer blocking, and after-hours blocking remain the same. When the transfer-to number matches the pattern for a blind transfer or park-slot transfer, Cisco Unified CME terminates the consultative call leg and transfers the call.

After the transfer-to digits are collected, if the transfer is not committed before the transfer-timeout expires in 30 seconds, the consultation call leg is disconnected.

These enhancements are supported only if:

- The **transfer-system full-consult** command (default) is set in telephony-service configuration mode.
- The **transfer-mode consult** command (default) is set for the transferor's directory number (ephone-dn).
- An idle line or channel is available for seizing, digit collection, and dialing.

Cisco Unified CME 4.3 and later versions enable these transfer enhancements by default.

To revert to the digit-collection method used in previous versions of Cisco Unified CME, see Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.

Consultative Transfer With Direct Station Select

Direct Station Select (DSS) is a feature that allows a multi-button phone user to transfer calls to an idle monitored line by pressing the Transfer key and the appropriate monitored line button. A monitored line is one that appears on two phones; one phone can use the line to make and receive calls and the other phone simply monitors whether the line is in use. For Cisco CME 3.2 and later versions, consultative transfers can occur during Direct Station Select (transferring calls to idle monitored lines).

If the person sharing the monitored line does not want to accept the call, the person announcing the call can reconnect to the incoming call by pressing the EndCall soft key to terminate the announcement call and pressing the Resume soft key to reconnect to the original caller.

Direct Station Select consultative transfer is enabled with the **transfer-system full-consult dss** command, which defines the call transfer method for all lines served by the router. The **transfer-system full-consult dss** command supports the **keep-conference** command. See Configure Conferencing, on page 1377.

H.450.2 and H.450.3 Support

H.450.2 is a standard protocol for exchanging call-transfer information across a network, and H.450.3 is a standard protocol for exchanging call-forwarding information across a network. Cisco CME 3.0 and later versions support the H.450.2 call-transfer standards and the H.450.3 call-forwarding standards that were introduced in Cisco ITS V2.1. Using the H.450.2 and H.450.3 standards to manage call transfer and forwarding in a VoIP network provides the following benefits:

- The final call path from the transferred party to the transfer destination is optimal, with no hairpinned routes or excessive use of resources.
- Call parameters (for example, codec) can be different for the different call legs.
- This solution is scalable.
- There is no limit to the number of times a call can be transferred.

Considerations for using the H.450.2 and H.450.3 standards include the following:

- Cisco IOS Release 12.2(15)T or a later release is required on all voice gateways in the network.
- Support of H.450.2 and H.450.3 is required on all voice gateways in the network. H.450.2 and H.450.3 are used regardless of whether the transfer-to or forward-to target is on the same Cisco Unified CME system as the transferring party or the forwarding party, so the transferred party must also support H.450.2 and the forwarded party must also support H.450.3. The exception is calls that can be reoriginated through hairpin call routing or through the use of an H.450 tandem gateway.

- Call forwarding over SIP networks uses the *302 Moved Temporarily* SIP response, which works in a manner similar to the way in which the H.450.3 standard is used for H.323 networks. To enable call forwarding, you must specify a pattern that matches the calling-party numbers of the calls that you want to be able to forward.
- Cisco Unified CME supports all SIP Refer method call transfer scenarios, but you must ensure that call transfer is enabled using H.450.2 standards.
- H.450 standards are not supported by Cisco Unified Communications Manager, Cisco BTS, or Cisco PGW, although hairpin call routing or an H.450 tandem gateway can be set up to handle calls to and from those types of systems.

The following series of figures depicts a call being transferred using H.450.2 standards. Figure 45: Call Transfer Using H.450.2: A Calls B, on page 1163 shows A calling B. Figure 46: Call Transfer Using H.450.2: B Consults with C, on page 1163 shows B consulting with C and putting A on hold. Figure 47: Call Transfer Using H.450.2: B Transfers A to C, on page 1163 shows that B has connected A and C, and Figure 48: Call

Transfer Using H.450.2: A and C Are Connected, on page 1163 shows A and C directly connected, with B no longer involved in the call.

Figure 45: Call Transfer Using H.450.2: A Calls B

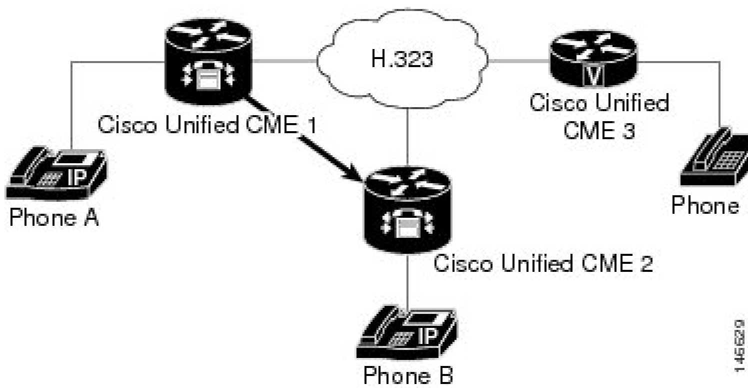


Figure 46: Call Transfer Using H.450.2: B Consults with C

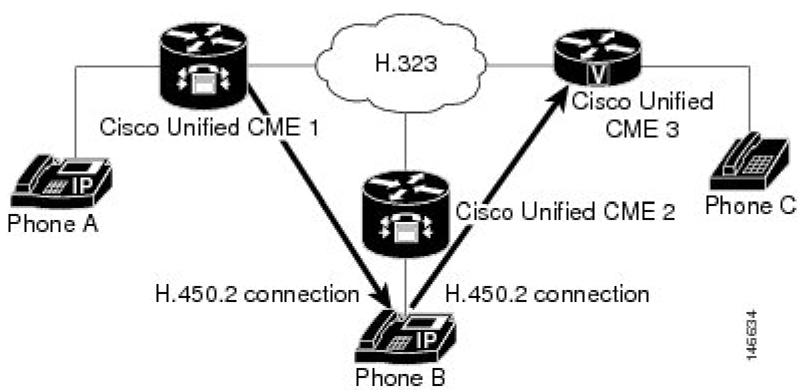


Figure 47: Call Transfer Using H.450.2: B Transfers A to C

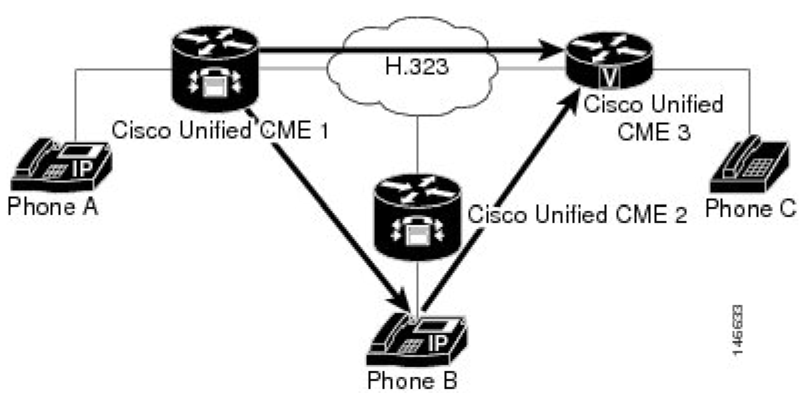
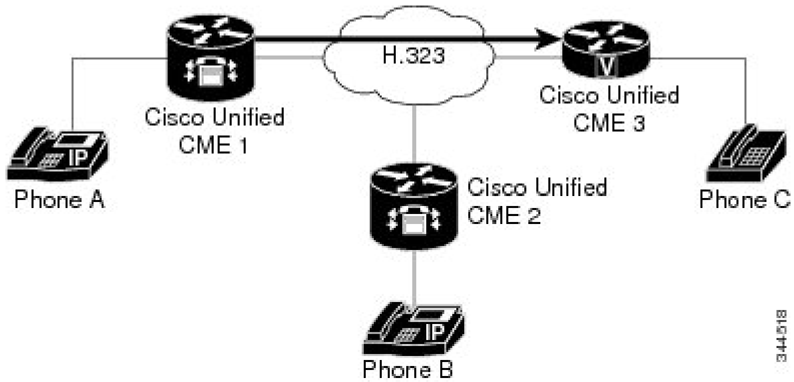


Figure 48: Call Transfer Using H.450.2: A and C Are Connected



Tips for Using H.450 Standards

Use H.450 standards when a network meets the following conditions:

- The router that you are configuring uses Cisco CME 3.0 or a later version, or Cisco ITS V2.1.
- For Cisco CME 3.0 or Cisco ITS V2.1 systems, all endpoints in the network must support H.450.2 and H.450.3 standards. For Cisco CME 3.1 or later systems, if some of the endpoints do not support H.450 standards (for example, Cisco Unified Communications Manager, Cisco BTS, or Cisco PGW), you can use hairpin call routing or an H.450 tandem gateway to handle transfers and forwards with those endpoints. Also, either you must explicitly disable H.450.2 and H.450.3 on the dial peers that handle those calls or you must enable H.450.12 capability to automatically detect the calls that support H.450.2 and H.450.3 and those calls that do not.

Support for the H.450.2 standard and the H.450.3 standard is enabled by default and can be disabled globally or for individual dial peers. For configuration information, see Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.

Transfer Method Recommendations by Cisco Unified CME Version

You must specify the method to use for call transfers: H.450.2 standard signaling or Cisco proprietary signaling, and whether transfers should be blind or allow consultation. Table 100: Transfer Method Recommendations, on page 1165 summarizes transfer method recommendations for all Cisco Unified CME versions.

Table 100: Transfer Method Recommendations

Cisco Unified CME Version	transfer-system Command Default	transfer-system Keyword to Use	Transfer Method Recommendation
4.0 and later	**full-consult**	**full-consult** or **full-blind**	Use H.450.2 for call transfer, which is the default for this version. You do not need to use the **transfer-system** command unless you want to use the **full-blind** or **dss** keyword. Optionally, you can use the proprietary Cisco method by using the **transfer-system** command with the **blind** or **local-consult** keyword. Use H.450.7 for call transfer using QSIG supplementary services
3.0 to 3.3	**blind**	**full-consult** or **full-blind**	Use H.450.2 for call transfer. You must explicitly configure the **transfer-system** command with the **full-consult** or **full-blind** keyword because H.450.2 is not the default for this version. Optionally, you can use the proprietary Cisco method by using the **transfer-system** command with the **blind** or **local-consult** keyword.

Cisco Unified CME Version	transfer-system Command Default	transfer-system Keyword to Use	Transfer Method Recommendation
2.1	**blind**	**blind** or **local-consult**	Use the Cisco proprietary method, which is the default for this version. You do not need to use the **transfer-system** command unless you want to use the **local-consult** keyword. Optionally, you can use the **transfer-system** command with the **full-consult** or **full-blind** keyword. You must also configure the router with a Tcl script that is contained in the app-h450-transfer.x.x.x.x.zip file. This file is available from the Cisco Unified CME software download website at: Download Software.
Earlier than 2.1	**blind**	**blind**	Use the Cisco proprietary method, which is the default for this version. You do not need to use the **transfer-system** command unless you want to use the **local-consult** keyword.

H.450.12 Support

Cisco CME 3.1 and later versions support the H.450.12 call capabilities standard, which provides a means to advertise and dynamically discover H.450.2 and H.450.3 capabilities in voice gateway endpoints on a call-by-call basis. When discovered, the calls associated with non-H.450 endpoints can be directed to use non-H.450 methods for transfer and forwarding, such as hairpin call routing or H.450 tandem gateway.

When H.450.12 is enabled, H.450.2 and H.450.3 services are disabled for call transfers and call forwards unless a positive H.450.12 indication is received from all other VoIP endpoints involved in the call. If a positive H.450.12 indication is received, the router uses the H.450.2 standard for call transfers and the H.450.3 standard for call forwarding. If a positive H.450.12 indication is not received, the router uses the alternative method that you have configured for call transfers and forwards, either hairpin call routing or an H.450 tandem gateway.

You can have either of the following situations in your network:

- All gateway endpoints support H.450.2 and H.450.3 standards. In this situation, no special configuration is required because support for H.450.2 and H.450.3 standards is enabled on the Cisco CME 3.1 or later router by default. H.450.12 capability is disabled by default, but it is not required because all calls can use H.450.2 and H.450.3 standards.
- Not all gateway endpoints support H.450.2 and H.450.3 standards. Therefore, specify how non-H.450 calls are to be handled by choosing one of the following options:
    - Enable the H.450.12 capability in Cisco CME 3.1 and later to dynamically determine, on a call-by-call basis, whether each call has H.450.2 and H.450.3 support. If H.450.12 is enabled and a call is determined to have H.450 support, the call is transferred using H.450.2 standards or forwarded using H.450.3 standards. See Enable H.450.12 Capabilities, on page 1196.
    Support for the H.450.12 standard is disabled by default and can be enabled globally or for individual dial peers.

      If the call does not have H.450 support, it can be handled by a VoIP-to-VoIP connection that you configure using dial peers and Enable H.323-to-H.323 Connection Capabilities, on page 1198. The connection can be used for hairpin call routing or routing to an H.450 tandem gateway.
    - Explicitly disable H.450.2 and H.450.3 capability on a global basis or by individual dial peer, which forces all calls to be handled by a VoIP-to-VoIP connection that you configure using dial peers and the Enable H.323-to-H.323 Connection Capabilities, on page 1198. This connection can be used for hairpin call routing or routing to an H.450 tandem gateway.

Hairpin Call Routing

Cisco CME 3.1 and later supports hairpin call routing using a VoIP-to-VoIP connection to transfer and forward calls that cannot use H.450 standards. When a call that originally terminated on a voice gateway is transferred or forwarded by a phone or other application attached to the gateway, the gateway reoriginates the call and routes the call as appropriate, making a VoIP-to-VoIP, or hairpin, connection. This approach avoids any protocol dependency on the far-end transferred-party endpoint or transfer-destination endpoint. Hairpin routing of transferred and forwarded calls also causes the generation of separate billing records for each call leg, so that the transferred or forwarded call leg is typically billed to the user who initiates the transfer or forward.

In Cisco CME 3.2 and later versions, transcoding between G.711 and G.729 is supported when one leg of a VoIP-to-VoIP hairpin call uses G.711 and the other leg uses G.729.

Hairpin call routing provides the following benefits:

- Call transfer and forwarding is provided to non-H.450 endpoints, such as Cisco Unified Communications Manager, Cisco BTS, or Cisco PGW.
- The network can also contain Cisco CME 3.0 or Cisco ITS 2.1 systems.

Hairpin call routing has the following disadvantages:

- End-to-end signaling and media delay are increased significantly.
- A single hairpinned call uses as much WAN bandwidth as two directly connected calls.

VoIP-to-VoIP hairpin connections can be made using dial peers if the **allow-connections h323 to h323** command is enabled and at least one of the following is true:

- H.450.12 is used to detect calls on which H.450.2 or H.450.3 is not supported by the remote system.
- H.450.2 or H.450.3 is explicitly disabled.
- Cisco Unified CME automatically detects that the remote system is a Cisco Unified Communications Manager.

Figure 49: Hairpin with H.323: A Calls B, on page 1169 shows a call that is made from A to B. Figure 50: Hairpin with H.323: Call is Forwarded to C, on page 1169 shows that B has forwarded all calls to C. Figure

51: Hairpin with H.323: A is Connected to C via B, on page 1169 shows that A and C are connected by an H.323 hairpin.

Figure 49: Hairpin with H.323: A Calls B

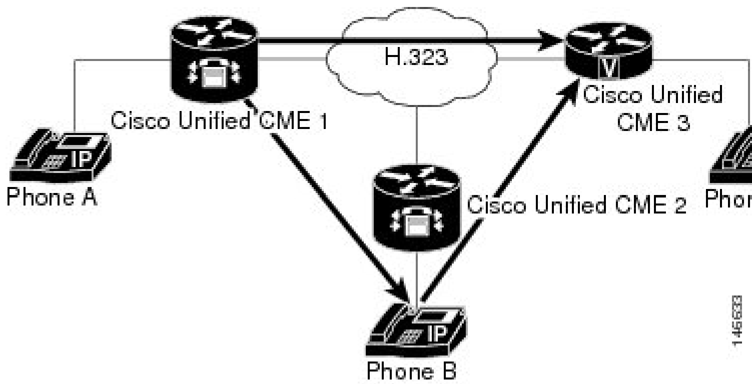


Figure 50: Hairpin with H.323: Call is Forwarded to C

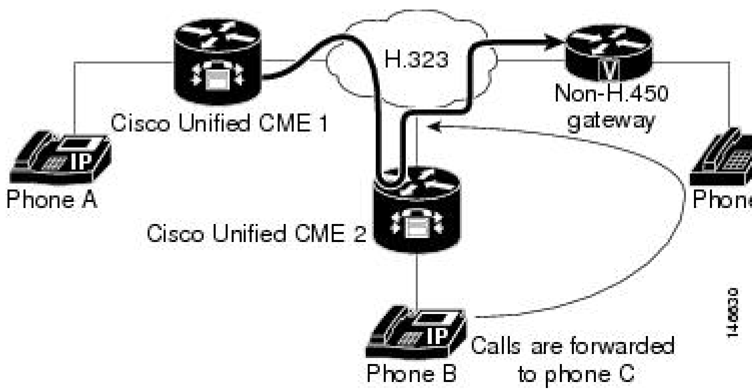
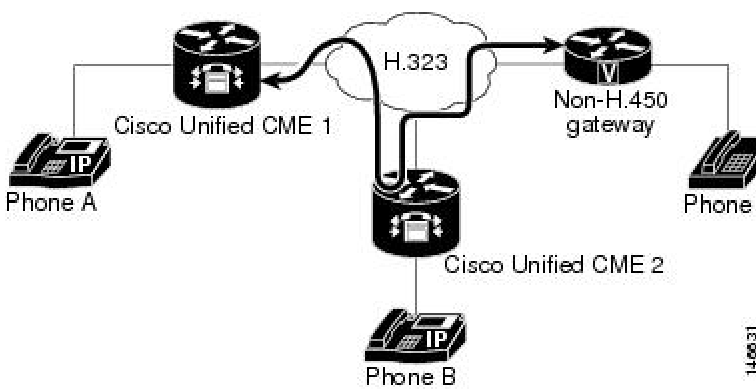


Figure 51: Hairpin with H.323: A is Connected to C via B



Tips for Using Hairpin Call Routing

Use hairpin call routing when a network meets the following three conditions:

- The router that you are configuring uses Cisco CME 3.1 or a later version.
- Some or all calls require VoIP-to-VoIP routing because they cannot use H.450 standards, which can happen for any of the following reasons:
    - H.450 capabilities have been explicitly disabled on the router.
    - H.450 capabilities do not exist in the network.
    - H.450 capabilities are supported on some endpoints and not supported on other endpoints, including those handled by Cisco Unified Communications Manager, Cisco BTS, and Cisco PGW. When some endpoints support H.450 and others do not, you must enable H.450.12 capabilities on the router to detect which endpoints are H.450-capable or designate some dial peers as H.450-capable. For more information about enabling H.450.12 capabilities, see Enable H.450.12 Capabilities, on page 1196.
- No voice gateway is available to act as an H.450 tandem gateway.

For information about configuring Cisco Unified CME to forward calls using local hairpin routing, see Forward Calls Using Local Hairpin Routing, on page 1200.

Support for VoIP-to-VoIP connections is disabled by default and can be enabled globally. For configuration information, see Enable H.323-to-H.323 Connection Capabilities, on page 1198.

Calling Number Local

In a scenario where calls are forwarded using local hairpin call routing, you can use the Calling Number Local feature. Calling Number Local replaces a calling-party number and name with the forwarding-party number and name (the local number and name). For ephone-dns, the CLI command **calling-number local** is configured under telephony-service configuration to enable the feature. For more information, see Cisco Unified Communications Manager Express Command Reference.

From Cisco Unified CME Release 12.0 onwards, calling number local feature is supported for voice register DNs as well. For voice register DNs, the CLI command **calling-number local** is configured in voice register global configuration mode. For more information, see Cisco Unified Communications Manager Express Command Reference.

When the CLI command **calling-number local** is enabled, the calling number is replaced with the forwarding party's number. If the forwarded number is over a trunk, toll charges may be applied on the forwarding number.

H.450 Tandem Gateways

H.450 tandem gateways address the limitations of hairpin call routing using a manner similar to hairpin call routing but without the double WAN link traversal created by hairpin connections. An H.450 tandem gateway is an additional voice gateway that serves as a “front-end” for a call processor that does not support the H.450 standards, such as Cisco Unified Communications Manager, Cisco BTS Softswitch (Cisco BTS), or Cisco PSTN Gateway (Cisco PGW). Transferred and forwarded calls that are intended for non-H.450 endpoints are terminated instead on the H.450 tandem gateway and reoriginated there for delivery to the non-H.450 endpoints. The H.450 tandem gateway can also serve as a PSTN gateway.

An H.450 tandem gateway is configured with a dial peer that points to the Cisco Unified Communications Manager or other system for which the H.450 tandem gateway is serving as a front end. The H.450 tandem voice gateway is also configured with dial peers that point to all the Cisco Unified CME systems in the private H.450 network. In this way, Cisco Unified CME and the Cisco Unified Communications Manager are not directly linked to each other, but are instead both linked to an H.450 tandem gateway that provides H.450 services to the non-H.450 platform.

An H.450 tandem gateway can also work as a PSTN gateway for remote Cisco Unified CME systems and for Cisco Unified Communications Manager (or other non-H.450 system). Use different inbound dial peers to separate Cisco Unified Communications Manager-to-PSTN G.711 calls from tandem gateway-to-Cisco Unified CME G.729 calls.

Note An H.450 tandem gateway that is used in a network to support non-H.450-capable call processing systems requires the Integrated Voice and Video Services feature license. This feature license, which was introduced in March 2004, includes functionality for H.323 gatekeeper, IP-to-IP Gateway, and H.450 tandem gateway. With Cisco IOS Release 12.3(7)T, an H.323 gatekeeper feature license is required with a JSX Cisco IOS image on the selected router. Consult your Cisco Unified CME SE regarding the required feature license. With Cisco IOS Release 12.3(7)T, you cannot use Cisco Unified CME and H.450 tandem gateway functionality on the same router.

VoIP-to-VoIP connections can be made for an H.450 tandem gateway if the **allow-connections h323 to h323** command is enabled and one or more of the following is true:

- H.450.12 is used to dynamically detect calls on which H.450.2 or H.450.3 is not supported by the remote VoIP system.
- H.450.2 or H.450.3 is explicitly disabled.
- Cisco CME 3.1 or later automatically detects that the remote system is a Cisco Unified Communications Manager.

For Cisco CME 3.1 and earlier, the only type of VoIP-to-VoIP connection supported by Cisco Unified CME is H.323-to-H.323. For Cisco CME 3.2 and later versions, H.323-to-SIP connections are allowed only for Cisco Unified CME systems running Cisco Unity Express.

Figure 52: H.450 Tandem Gateway, on page 1172 shows a tandem voice gateway that is located between the central hub of the network of a CPE-based Cisco CME 3.1 or later network and a Cisco Unified Communications Manager network. This topology would work equally well with a Cisco BTS or Cisco PGW in place of the Cisco Unified Communications Manager.

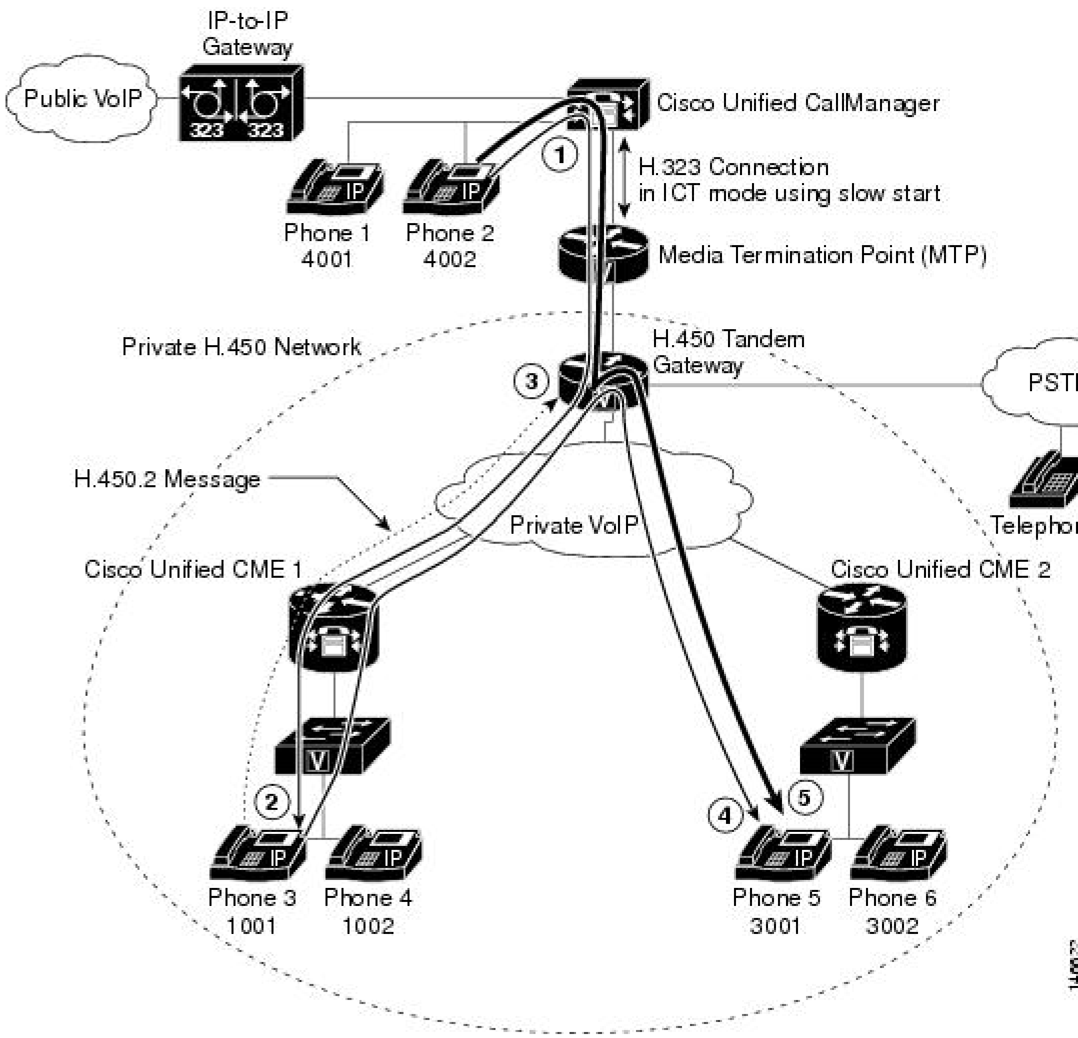
In the network topology in Figure 52: H.450 Tandem Gateway, on page 1172, the following events occur (refer to the event numbers on the illustration):

1. A call is generated from extension 4002 on phone 2, which is connected to a Cisco Unified Communications Manager. The H.450 tandem gateway receives the H.323 call and, acting as the H.323 endpoint, the H.450 tandem gateway handles the call connection to a Cisco Unified IP phone in a CPE-based Cisco CME 3.1 or later network.
2. The call is received by extension 1001 on phone 3, which is connected to Cisco Unified CME 1. Extension 1001 performs a consultation transfer to extension 2001 on phone 5, which is connected to Cisco Unified CME 2.
3. When extension 1001 transfers the call, the H.450 tandem gateway receives an H.450.2 message from extension 1001.

4 The H.450 tandem gateway terminates the call leg from extension 1001 and reoriginates a call leg to extension 2001, which is connected to Cisco Unified CME 2.

5 Extension 4002 is connected with extension 2001.

Figure 52: H.450 Tandem Gateway



Tips for Using H.450 Tandem Gateways

Use this procedure when a network meets the following conditions:

- The router that you are configuring uses Cisco CME 3.1 or a later version.
- Some endpoints in the network are not H.450-capable, including those handled by Cisco Unified Communications Manager, Cisco BTS, and Cisco PGW.

Support for VoIP-to-VoIP connections is disabled by default and can be enabled globally. For more information, see Enable H.323-to-H.323 Connection Capabilities, on page 1198.

Use dial peers to set up an H.450 tandem gateway. See Dial Peers, on page 1173.

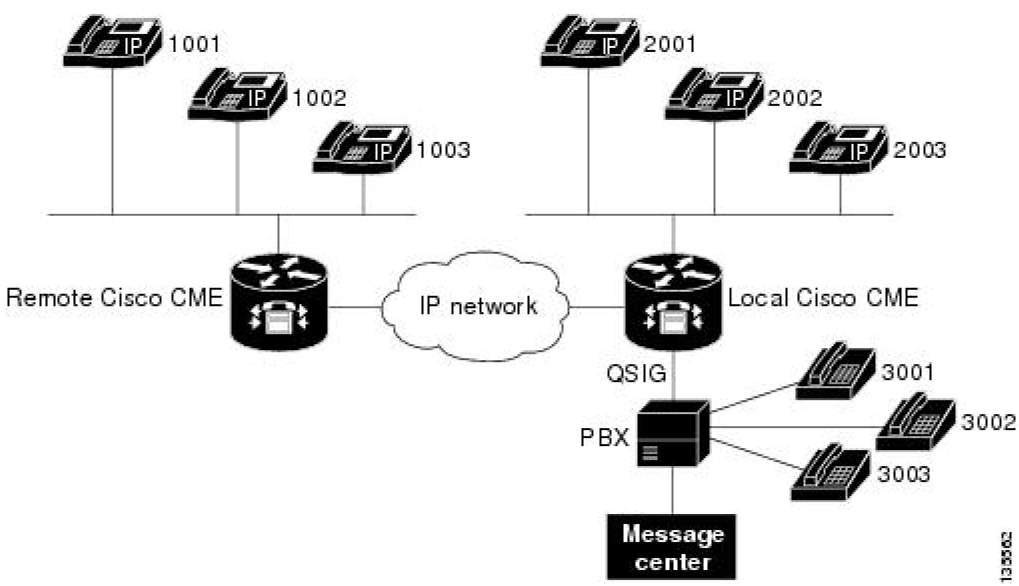
Dial Peers

Dial peers describe the virtual interfaces to or from which a call is established. All voice technologies use dial peers to define the characteristics associated with a call leg. Attributes applied to a call leg include specific quality of service (QoS) features, compression/decompression (codec), voice activity detection (VAD), and fax rate. Dial peers are also used to establish the routing paths in your network, including special routing paths such as hairpins and H.450 tandem gateways. Dial peer settings override the global settings for call forward and call transfer.

Q Signaling Supplementary Services

Q Signaling (QSIG) is an intelligent inter-PBX signaling system widely adopted by PBX vendors. It supports a range of basic services, generic functional procedures, and supplementary services. Cisco Unified CME 4.0 introduces supplementary services features that allow Cisco Unified CME phones to seamlessly interwork using QSIG with phones connected to a PBX. One benefit is that IP phones can use a PBX message center with proper MWI notifications. Figure 53: Cisco Unified CME System with PBX, on page 1173 illustrates a topology for a Cisco Unified CME system with some phones under the control of a PBX.

Figure 53: Cisco Unified CME System with PBX



The following QSIG supplementary service features are supported in Cisco Unified CME systems. They follow the standards from the European Computer Manufacturers Association (ECMA) and the International Organization for Standardization (ISO) on PRI and BRI interfaces.

- Basic calls between IP phones and PBX phones.
- Calling Line/Name identification (CLIP/CNIP) presented on an IP phone when called by a PBX phone; in the reverse direction, such information is provided to the called endpoint.

- Connected Line/Name identification (COLP/CONP) information provided when a PBX phone calls an IP phone and is connected; in the reverse direction, such information presented on an IP phone.
- Call Forward using QSIG and H.450.3 to support any combination of IP phone and PBX phone, including an IP phone in the Cisco Unified CME system that is connected to a PBX or an IP phone in another Cisco Unified CME system across an H.323 network.
- Call forward to the PBX message center according to the configured policy. The other two endpoints can be a mixture of IP phone and PBX phones.
- Hairpin call transfer, which interworks with a PBX in transfer-by-join mode. Note that Cisco Unified CME does not support the actual signaling specified for this transfer mode (including the involved FACILITY message service APDUs) which are intended for an informative purpose only and not for the transfer functionality itself. As a transferrer (XOR) host, Cisco Unified CME simply hairpins two call legs to create a connection; as a transferee (XEE) or transfer-to (XTO) host, it will not be aware of a transfer that is taking place on an existing leg. As a result, the final endpoint may not be updated with the accurate identity of its peer. Both blind transfer and consult transfer are supported.
- Message-waiting indicator (MWI) activation or deactivation requests are processed from the PBX message center.
- The PBX message center can be interrogated for the MWI status of a particular ephone-dn.
- A user can retrieve voice messages from a PBX message center by making a normal call to the message center access number.

For information about enabling QSIG supplementary services, see Enable H.450.7 and QSIG Supplementary Services at System-Level, on page 1202 and Enable H.450.7 and QSIG Supplementary Services on a Dial Peer, on page 1204.

Disable SIP Supplementary Services for Call Forward and Call Transfer

If a destination gateway does not support supplementary services, you can disable REFER messages for call transfers and the redirect responses for call forwarding from being sent by Cisco Unified CME.

For configuration information, see Disable SIP Supplementary Services for Call Forward and Call Transfer, on page 1206.

Typical Network Scenarios for Call Transfer and Call Forwarding

In a mixed network that involves two or more types of call agents or call-control systems, there can be communication protocol discrepancies and dependencies, and therefore the opportunity for interoperability errors. These discrepancies show up most often when a call is being transferred or forwarded. This section provides descriptions of the specific mixed-network scenarios you might encounter when configuring a router running Cisco CME 3.1 or a later version. Each of the following sections point to the configuration instructions necessary to ensure call transfer and forwarding capabilities throughout the network.

Note Cisco Communications Manager Express 3.2 (Cisco CME 3.2) and later versions provide full call-transfer and call-forwarding with call processing systems on the network that support H.450.2, H.450.3, and H.450.12 standards. For interoperability with call processing systems that do not support H.450 standards, Cisco CME 3.2 and later versions provide VoIP-to-VoIP hairpin call routing without requiring the special Tool Command Language (Tcl) script that was needed in earlier versions of Cisco Unified CME.

Cisco CME 3.1 or Later and Cisco IOS Gateways

In a network with Cisco CME 3.1 or a later version and Cisco IOS gateways, all systems that might participate in calls that involve call transfer and call forwarding are capable of supporting the H.450.2, H.450.3, and H.450.12 standards. This is the simplest environment for operating the Cisco CME 3.1 or later features.

Configuration for this type of network consists of:

1. Setting up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.
2. Enabling H.450.12 globally to detect any calls on which H.450.2 and H.450.3 standards are not supported. Although this step is optional, we recommend it. See Enable H.450.12 Capabilities, on page 1196.
3. Optionally setting up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route calls that do not support H.450.2 or H.450.3 standards. See Enable H.323-to-H.323 Connection Capabilities, on page 1198.
4. Setting up dial peers to manage call legs within the network.

Cisco CME 3.0 or an Earlier Version and Cisco IOS Gateways

Before Cisco CME 3.1, H.450.2 and H.450.3 standards are used for all calls by default and routers do not support the H.450.12 standard.

Configuration for this type of network consists of:

- Setting up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178
- Enabling H.450.12 in advertise-only mode on Cisco CME 3.1 or later systems. As each Cisco CME 3.0 system is upgraded to Cisco CME 3.1 or later, enable H.450.12 in advertise-only mode. Note that no checking for H.450.2 or H.450.3 support is done in advertise-only mode. When all Cisco CME 3.0 systems in the network have been upgraded to Cisco CME 3.1 or later, remove the advertise-only restriction. See Enable H.450.12 Capabilities, on page 1196
- Optionally setting up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route calls that cannot use H.450.2 or H.450.3 standards. See Enable H.323-to-H.323 Connection Capabilities, on page 1198
- Setting up dial peers to manage call legs within the network.

Cisco CME 3.1 or Later, Non-H.450 Gateways, and Cisco IOS Gateways

In a network with Cisco CME 3.1 or later, non-H.450 gateways, and Cisco IOS gateways, the H.450.2 and H.450.3 services are provided only to calling endpoints that use H.450.12 to explicitly indicate that they are capable of H.450.2 and H.450.3 operations. Because the Cisco BTS and Cisco PGW do not support the H.450.12 standard, calls to and from these systems that involve call transfer or forwarding are handled using H.323-to-H.323 hairpin call routing.

Configuration for this type of network consists of:

1 Setting up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). Optionally disable H.450.2 and H.450.3 capabilities on dial peers that point to non-H.450-capable systems such as Cisco Unified Communications Manager, Cisco BTS, or Cisco PGW. See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.
2 Enabling H.450.12 to detect any calls on which H.450.2 and H.450.3 standards are not supported, either globally or for specific dial peers. See Enable H.450.12 Capabilities, on page 1196.
3 Setting up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route calls that do not support H.450.2 or H.450.3 standards. See Enable H.323-to-H.323 Connection Capabilities, on page 1198.
4 Setting up dial peers to manage call legs within the network.

Note If your network contains a Cisco Unified Communications Manager, also see the instructions in the Enable Interworking with Cisco Unified Communications Manager, on page 1207.

Cisco Unified CME, Non-H.450 Gateways, and Cisco IOS Gateways

Note Cisco CME 3.0 and Cisco ITS V2.1 systems do not have H.450.12 capabilities.

In a network that contains a mix of Cisco Unified CME versions and at least one non-H.450 gateway, the simplest configuration approach is to globally disable all H.450.2 and H.450.3 services and force H.323-to-H.323 hairpin call routing for all transferred and forwarded calls. In this case, you would enable H.450.12 detection capabilities globally. Alternatively, you could select to enable H.450.12 capability for specific dial peers. In this case, you would not configure H.450.12 capability globally; you would leave it in its default disabled state.

Configuration for this type of network consists of:

1 Setting up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.
2 Enabling H.450.12 to detect any calls on which H.450.2 and H.450.3 standards are not supported, either globally or on specific dial peers. See Enable H.450.12 Capabilities, on page 1196
3 Setting up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route all transferred and forwarded calls. See Enable H.323-to-H.323 Connection Capabilities, on page 1198.
4 Setting up dial peers to manage call legs within the network.

Note If your network contains a Cisco Unified Communications Manager, also see the instructions in the Enable Interworking with Cisco Unified Communications Manager, on page 1207.

Cisco CME 3.1 or Later, Cisco Unified Communications Manager, and Cisco IOS Gateways

In a network with Cisco CME 3.1 or later, Cisco Unified Communications Manager, and Cisco IOS gateways, Cisco CME 3.1 and later versions support automatic detection of calls to and from Cisco Unified Communications Manager using proprietary signaling elements that are included with the standard H.323 message exchanges. The Cisco CME 3.1 or later system uses these detection results to determine the H.450.2 and H.450.3 capabilities of calls rather than using H.450.12 supplementary services capabilities exchange, which Cisco Unified Communications Manager does not support. If a call is detected to be coming from or going to a Cisco Unified Communications Manager endpoint, the call is treated as a non-H.450 call. All other calls in this type of network are treated as though they support H.450 standards. Therefore, this type of network should contain only Cisco CME 3.1 or later and Cisco Unified Communications Manager call-processing systems.

Configuration for this type of network consists of:

1. Setting up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178
2. Enabling H.450.12 to detect any calls on which H.450.2 and H.450.3 standards are not supported, either globally or on specific dial peers. See Enable H.450.12 Capabilities, on page 1196
3. Setting up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route all transferred and forwarded calls that are detected as being to or from Cisco Unified Communications Manager. SeeEnable H.323-to-H.323 Connection Capabilities, on page 1198
4. Setting up specific parameters for Cisco Unified Communications Manager. SeeEnable Cisco Unified Communications Manager to Interwork with Cisco Unified CME, on page 1212
5. Setting up dial peers to manage call legs within the network.

Cisco CME 3.0 or an Earlier Version, Cisco Unified Communications Manager, and Cisco IOS Gateways

Calls between the Cisco Unified Communications Manager and the older Cisco CME 3.0 or Cisco ITS V2.1 networks need special consideration. Because Cisco CME 3.0 and Cisco ITS V2.1 systems do not support automatic Cisco Unified Communications Manager detection and also do not natively support H.323-to-H.323 call routing, alternative arrangements are required for these systems.

To configure call transfer and forwarding on the Cisco CME 3.0 router, you can select from the following three options:

- Use a Tcl script to handle call transfer and forwarding by invoking Tcl-script-based H.323-to-H.323 hairpin call routing (app-h450-transfer.2.0.0.9.tcl or a later version). Enable this script on all VoIP dial peers and also under telephony-service mode, and set the local-hairpin script parameter to 1.
- Use a loopback-dn mechanism.
- Configure a loopback call path using router physical voice ports.

All three options force use of H.323-to-H.323 hairpin call routing for all calls regardless of whether the call is from a Cisco Unified Communications Manager or other H.323 endpoint (including Cisco CME 3.1 or later).

Configure Call Transfer and Forwarding

Enable Call Transfer and Forwarding on SCCP Phones at System-Level

To enable H.450 call transfers and forwards for transferring or forwarding parties; that is, to allow transfers and forwards to be initiated from a Cisco Unified CME system, perform the following steps.

Note H.450.2 and H.450.3 capabilities are enabled by default for transferred or forwarded parties and transfer-destination or forward-destination parties. Dial peer settings override the global setting.

Restriction

- Call transfers are handled differently depending on the Cisco Unified CME version. See Transfer Method Recommendations by Cisco Unified CME Version, on page 1164 for recommendations on selecting a transfer method for your Cisco Unified CME version.
- The **transfer-system local-consult** command is not supported if the transfer-to destination is on the Cisco ATA, Cisco VG224, or a SCCP-controlled FXS port.
- The H.450.2 and H.450.3 standards are not supported by Cisco Unified Communications Manager, Cisco BTS, or Cisco PGW.
- In versions earlier than Cisco Unified CME 4.2, the caller ID displays correctly only after connect; caller ID does not display correctly at Call Transfer or Call Forward.

Call-Transfer Recall

- Requires Cisco Unified CME 4.3 or a later version.
- Transferor and transfer-to party must be on the same Cisco Unified CME router; transferee party can be remote to the Cisco Unified CME router.
- Transfer recall is not supported if the transfer-to party has Call Forward Busy enabled, or if the transfer-to party is a hunt group pilot number.
- If the transfer-to party has Call Forward No Answer enabled, Cisco Unified CME recalls a transferred call only if the transfer-recall timeout is set to less than the timeout value set with the **call-forward noan** command.
- Recall timer for trunk-line directory number has precedence (set on transferor using **trunk** command with **transfer-timeout** keyword) over the transfer-recall timer. Transfer recall is not initiated for hairpin transfers.

Before You Begin

Cisco CME 3.0 or a later version, or Cisco ITS V2.1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **transfer-system**{**blind** | **full-blind** | **full-consult** [**dss**] | **local-consult** }
5. **transfer-pattern** *transfer-pattern* [**blind**]
6. **call-forward pattern** *pattern*
7. **timeouts transfer-recall** *seconds*
8. **transfer-digit-collect** {**new-call** | **orig-call**}
9. **exit**
10. **voice service voip**
11. **supplementary-service h450.2**
12. **supplementary-service h450.3**
13. **exit**
14. **dial-peer voice** *tag* **voip**
15. **supplementary-service h450.2**
16. **supplementary-service h450.3**
17. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**transfer-system**{**blind** | **full-blind** | **full-consult** [**dss**] | **local-consult** } **Example:** `Router(config-telephony)# transfer-system full-consult`	Specifies the call transfer method. • **blind—**Calls are transferred without consultation using the Cisco proprietary method and a single phone line. This is the default in versions earlier than Cisco Unified CME 4.0. • **full-blind—**Calls are transferred without consultation using H.450.2 standard methods.

	Command or Action	Purpose
		• **full-consult**—Calls are transferred with consultation using H.450.2 standard methods and a second phone line if available. Calls fall back to full-blind if the second line is unavailable. This is the default in Cisco Unified CME 4.0 and later versions. Transfer-system needs to be set at full-consult for the "transfer by directory" to work. Transfer by directory is supported by full-consult or blind transfer. If you want to transfer using directory/placed/missed/received calls, the transfer-system needs to be set at full-consult for this to work appropriately. When changed to full-consult, you can do "blind transfer" by selecting the number from the directory and when the other phone rings, you can press the softkey "Transfer" and the call will be transferred to the number selected and then you can hang up. • **dss**—(Optional) Calls are transferred with consultation to idle monitored lines. All other call-transfer behavior is identical to full-consult. • **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. Not supported if transfer-to destination is on the Cisco ATA, Cisco VG224, or a SCCP-controlled FXS port. • Cisco CME 3.0 and later versions—Use only the **full-blind** or **full-consult** keyword. • Before Cisco CME 3.0—Use the **local-consult** or **blind** keyword. (Cisco ITS 2.1 can use the **full-blind** or **full-consult** keyword by also using the Tcl script in the file called app-h450-transfer.x.x.x.x.zip.)
Step 5	**transfer-pattern** *transfer-pattern* [**blind**] **Example:** `Router(config-telephony)# transfer-pattern .T`	Allows transfer of telephone calls by Cisco Unified IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones. • *transfer-pattern*—String of digits for permitted call transfers. Wildcards are allowed. A pattern of .T transfers all calling parties using the H.450.2 standard. • **blind**—(Optional) When H.450.2 consultative call transfer is configured, forces transfers that match the pattern specified in this command to be executed as blind transfers. Overrides settings made using the **transfer-system** and **transfer-mode** commands.

	Command or Action	Purpose
		Note For transfers to nonlocal numbers, transfer-pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated.
Step 6	**call-forward pattern** *pattern* **Example:** `Router(config-telephony)# call-forward pattern .T`	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. Calling-party numbers that do not match the patterns defined with this command are forwarded using Cisco proprietary call forwarding for backward compatibility. **Note** For forwarding to nonlocal numbers, pattern matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated.
Step 7	**timeouts transfer-recall** *seconds* **Example:** `Router(config-telephony)# timeouts transfer-recall 30`	(Optional) Enables Cisco Unified CME to recall a transferred call if the transfer-to party is busy or does not answer. • *seconds*—Duration, in seconds, to wait before recalling a transferred call. Range: 1 to 1800. Default: 0 (disabled). This command is supported in Cisco Unified CME 4.3 and later versions. This command can also be configured in ephone-dn and ephone-dn-template configuration mode.
Step 8	**transfer-digit-collect** {**new-call** | **orig-call**} **Example:** `Router(config-telephony)# transfer-digit-collect orig-call`	(Optional) Selects the digit-collection method used for consultative call transfers. • **new-call**—Digits are collected from the new call leg. Default value in Cisco Unified CME 4.3 and later versions. • **orig-call**—Digits are collected from original call-leg. Default behavior in versions earlier than Cisco Unified CME 4.3. This command is supported in Cisco Unified CME 4.3 and later versions.
Step 9	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.

	Command or Action	Purpose
Step 10	**voice service voip** **Example:** `Router(config)# voice service voip`	(Optional) Enters voice-service configuration mode to establish global call transfer and forwarding parameters.
Step 11	**supplementary-service h450.2** **Example:** `Router(conf-voi-serv)# supplementary-service h450.2`	(Optional) Enables H.450.2 supplementary services capabilities globally. Default is enabled. Use the **no** form of this command to disable H.450.2 capabilities globally. You can also use this command in dial-peer configuration mode to enable H.450.2 services for a single dial peer.
Step 12	**supplementary-service h450.3** **Example:** `Router(conf-voi-serv)# supplementary-service h450.3`	(Optional) Enables H.450.3 supplementary services capabilities globally. Default is enabled. Use the **no** form of this command to disable H.450.3 capabilities globally. You can also use this command in dial-peer configuration mode to enable H.450.3 services for a single dial peer.
Step 13	**exit** **Example:** `Router(conf-voi-serv)# exit`	(Optional) Exits voice-service configuration mode.
Step 14	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	(Optional) Enters dial-peer configuration mode.
Step 15	**supplementary-service h450.2** **Example:** `Router(config-dial-peer)# no supplementary-service h450.2`	(Optional) Enables H.450.2 supplementary services capabilities for an individual dial peer. Default is enabled. You can also use this command in voice-service configuration mode to enable H.450.2 services globally. • If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default. • If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. • If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.
Step 16	**supplementary-service h450.3** **Example:** `Router(config-dial-peer)# no supplementary-service h450.3`	(Optional) Enables H.450.3 supplementary services capabilities exchange for an individual dial peer.

	Command or Action	Purpose
		Default is enabled. You can also use this command in voice-service configuration mode to enable H.450.3 services globally. • If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default configuration. • If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. • If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.
Step 17	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Enable Call-Transfer Recall on SIP Phones at System-Level

To enable call-transfer recalls to be initiated from a Cisco Unified CME system, perform the following steps.

Note

- Transferor and transfer-to party must be on the same Cisco Unified CME router; transferee party can be remote to the Cisco Unified CME router.
- Transfer recall is not supported if the transfer-to party has Call Forward Busy enabled, or if the transfer-to party is a hunt group pilot number.

Before You Begin

Cisco Unified CME 11.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **timeouts transfer-recall** *seconds*
5. **exit**
6. **voice service voip**
7. **no supplementary-service sip refer**
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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.

Step 4	**timeouts transfer-recall** *seconds*
	
	Example:
	`Router(config-register-global)# timeouts transfer-recall 30`
	`Router(config-register-dn)# timeouts transfer-recall 30`
		Enables Cisco Unified CME to recall a transferred call if the transfer-to party is busy or does not answer in the voice register global configuration mode. You can also recall a transferred call in the voice register dn configuration mode.
		• *seconds*—Duration, in seconds, to wait before recalling a transferred call. Range: 1 to 1800. Default: 0 (disabled).
		• This command is supported in Cisco Unified CME 11.6 and later versions.
		• This command can also be configured in voice register dn or voice register global configuration modes.

Step 5	**exit** **Example:** `Router(config-register-global)# exit`	Exits voice register global configuration mode.

	Command or Action	Purpose
Step 6	**voice service voip** **Example:** `Router(config)# voice service voip`	(Optional) Enters voice-service configuration mode.
Step 7	**no supplementary-service sip refer** **Example:** `Router(config-voi-serv)# no supplementary-service sip refer`	Prevents the router from forwarding a REFER message to the destination for call-transfer recalls.
Step 8	**end** **Example:** `Router(config-voi-serv)# end`	Returns to privileged EXEC mode.

Enable Call Forwarding for a Directory Number

To define the conditions and target numbers for call forwarding for individual ephone-dns, and set other restrictions for call forwarding, perform the following steps.

Note When defining call forwarding to nonlocal numbers, it is important to note that pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated.

Restriction

- Call forwarding is invoked only if that phone is dialed directly. Call forwarding is not invoked when the phone number is called through a sequential, longest-idle, or peer hunt group.
- If call forwarding is configured for hunt group member, call forward is ignored by the hunt group.
- Calls from an internal extension to an extension which is busy, is forwarded to the SNR destination even if no forward local-calls is configured under the Directory Number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **call-forward pattern** *pattern*
5. **exit**
6. **ephone-dn** *dn-tag* [**dual-line**]
7. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
8. **call-forward all** *target-number*
9. **call-forward busy** *target-number* [**primary** | **secondary**] [**dialplan-pattern**]
10. **call-forward noan** *target-number* **timeout** *seconds* [**primary** | **secondary**] [**dialplan-pattern**]
11. **call-forward night-service** *target-number*
12. **call-forward max-length** *length*
13. **no forward local-calls**
14. **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	**telephony-service** **Example:** `Router(config)#`	Enters telephony-service configuration mode.
Step 4	**call-forward pattern** *pattern* **Example:** `Router(config-telephony)# call-forward pattern .T`	Specifies the H.450.3 standard for call forwarding. Calling-party numbers that do not match the patterns defined with this command are forwarded using Cisco-proprietary call forwarding for backward compatibility. • *pattern*—Digits to match for call forwarding using the H.450.3 standard. If an incoming calling-party number matches the pattern, it is forwarded using the H.450.3 standard. A pattern of .T forwards all calling parties using the H.450.3 standard.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 6	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 20`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. • **dual-line**—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.
Step 7	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 2777 secondary 2778`	Configures a valid extension number for this ephone-dn instance.
Step 8	**call-forward all** *target-number* **Example:** `Router(config-ephone-dn)# call-forward all 2411`	Forwards all calls for this extension to the specified number. • *target-number*—Phone number to which calls are forwarded. **Note** After you use this command to specify a target number, the phone user can activate and cancel the call-forward-all state from the phone using the CFwdAll soft key or a feature access code (FAC).
Step 9	**call-forward busy** *target-number* [**primary** | **secondary**] [**dialplan-pattern**] **Example:** `Router(config-ephone-dn)# call-forward busy 2513`	Forwards calls for a busy extension to the specified number.
Step 10	**call-forward noan** *target-number* **timeout** *seconds* [**primary** | **secondary**] [**dialplan-pattern**] **Example:** `Router(config-ephone-dn)# call-forward noan 2513 timeout 45`	Forwards calls for an extension that does not answer.
Step 11	**call-forward night-service** *target-number* **Example:** `Router(config-ephone-dn)# call-forward night-service 2879`	Automatically forwards incoming calls to the specified number when night service is active. • *target-number*—Phone number to which calls are forwarded. **Note** Night service must also be configured. See Configure Call Coverage Features, on page 1278.

	Command or Action	Purpose
Step 12	**call-forward max-length** *length* **Example:** `Router(config-ephone-dn)# call-forward max-length 5`	(Optional) Limits the number of digits that can be entered for a target number when using the CfwdAll soft key on an IP phone. • *length*—Number of digits that can be entered using the CfwdAll soft key on an IP phone.
Step 13	**no forward local-calls** **Example:** `Router(config-ephone-dn)# no forward local-calls`	(Optional) Specifies that local calls (calls from ephone-dns on the same Cisco Unified CME system) will not be forwarded from this extension. • If this extension is busy, an internal caller hears a busy signal. • If this extension does not answer, the internal caller hears ringback.
Step 14	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Call Transfer for a Directory Number

To enable call transfer for a specific directory number, perform the following steps. This procedure overrides the global setting for blind or consultative transfer for individual directory numbers.

Before You Begin

Call transfer must be enabled globally. See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **transfer-mode** {**blind** | **consult**}
5. **timeouts transfer-recall** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 20`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. • **dual-line**—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.
Step 4	**transfer-mode** {**blind** | **consult**} **Example:** `Router(config-ephone-dn)# transfer-mode blind`	Specifies the type of call transfer for an individual directory number using the H.450.2 standard, allowing you to override the global setting. • Default: system-level value set with the **transfer-system** command.
Step 5	**timeouts transfer-recall** *seconds* **Example:** `Router(config-ephone-dn)# timeouts transfer-recall 30`	(Optional) Enables call-transfer recall and sets the number of seconds that Cisco Unified CME waits before recalling a transferred call if the transfer-to party does not answer or is busy. • *seconds*—Duration, in seconds, to wait before recalling a transferred call. Range: 1 to 1800. Default: 0 (disabled). • This command is supported in Cisco Unified CME 4.3 and later versions. • This command can also be configured in ephone-dn-template and telephony-service configuration mode.
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Configure Call Transfer Options for SCCP Phones

To specify a maximum number of digits for transfer destinations or block transfers to external destinations by individual phones, perform the following steps.

Before You Begin

- Transfers made to speed-dial numbers are not blocked when the **transfer-pattern blocked** command is used.

- Transfers made using speed-dial are not blocked by the **after-hours block pattern** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **transfer-pattern blocked**
5. **transfer max-length** *digit-length*
6. **exit**
7. **ephone** *phone-tag*
8. **ephone-template** *template-tag*
9. **restart**
10. **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-template** *template-tag* **Example:** `Router(config)# ephone-template 1`	Enters ephone-template configuration mode. • *template-tag*—Unique number that identifies this template during configuration tasks. Range: 1 to 20.
Step 4	**transfer-pattern blocked** **Example:** `Router(config-ephone-template)# transfer-pattern blocked`	(Optional) Prevents directory numbers on the phone to which this template is applied from transferring calls to patterns specified in the **transfer-pattern** (telephony-service) command. **Note** This command is also available in ephone configuration mode to block external transfers from individual phones without using a template.
Step 5	**transfer max-length** *digit-length* **Example:** `Router(config-ephone-template)# transfer max-length 8`	(Optional) Specifies the maximum number of digits the user can dial when transferring a call. • *digit-length*—Number of digits allowed in a number to which a call is being transferred. Range: 3 to 16. Default: 16.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 7	**ephone** *phone-tag* **Example:** `Router(config)# ephone 25`	Enters ephone configuration mode.
Step 8	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 1`	Applies a template to a phone. • *template-tag*—Template number that you want to apply to this phone.
Step 9	**restart** **Example:** `Router(config-ephone)# restart`	Performs a fast reboot of this phone without contacting the DHCP server for updated information. Repeat Step 6 to Step 9 for each phone on which you want to limit transfer capabilities.
Step 10	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Verify Call Transfer for SCCP Phones

Step 1 Use the **show running-config** command to verify your configuration. Transfer method and patterns are listed in the telephony-service portion of the output. You can also use the **show telephony-service** command to display this information.

Example:

```
Router# show running-config
!
telephony-service
fxo hook-flash
load 7910 P00403020214
load 7960-7940 P00305000600
load 7914 S00103020002
load 7905 CP7905040000SCCP040701A
max-ephones 100
max-dn 500
ip source-address 10.115.33.177 port 2000
max-redirect 20
no service directed-pickup
timeouts ringing 10
voicemail 7189
max-conferences 8 gain -6
moh music-on-hold.au
```

```
web admin system name cisco password cisco
dn-webedit
time-webedit
transfer-system full-consult
transfer-pattern 92......
transfer-pattern 91.........
transfer-pattern 93......
transfer-pattern 94......
transfer-pattern 95......
transfer-pattern 96......
transfer-pattern 97......
transfer-pattern 98......
transfer-pattern 99......
transfer-pattern .T
secondary-dialtone 9
!
create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
```

Step 2 If you have used the **transfer-mode** command to override the global transfer mode for an individual ephone-dn, use the **show running-config** or **show telephony-service ephone-dn** command to verify that setting.

Example:

```
Router# show running-config
!
ephone-dn 40 dual-line
number 451
description Main Number
huntstop channel
no huntstop
transfer-mode blind
```

Step 3 Use the **show telephony-service ephone-template** command to view ephone-template configurations.

Specify Transfer Patterns for Trunk-to-Trunk Calls and Conferences for SIP

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

Before You Begin

Cisco Unified CME 9.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **transfer-pattern** *transfer-pattern*
5. **exit**
6. Enter one of the following commands:
    - **voice register pool** *pool-tag*
    - **voice register template** *template-tag*
    - **ephone** *phone tag*
    - **ephone-template** *template-tag*
7. **transfer max-length** *max-length*
8. **exit**
9. **telephony-service**
10. **conference transfer-pattern**
11. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode for configuring Cisco Unified CME.
Step 4	**transfer-pattern** *transfer-pattern* **Example:** `Router(config-telephony)# transfer-pattern 1234...Router(config-telephony)# transfer-pattern 2468..`	Allows the transfer of calls from Cisco IP phones to specified directory numbers of phones other than Cisco IP phones. • *transfer-pattern*—String of digits for permitted call transfers. Wildcards are allowed. A maximum of 32 transfer patterns can be entered, using a separate command for each one.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode and enters global configuration mode.
Step 6	Enter one of the following commands: • **voice register pool** *pool-tag* • **voice register template** *template-tag* • **ephone** *phone tag* • **ephone-template** *template-tag* **Example:** `Router(config)# voice register pool 25`	Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME or for a set of Cisco Unified SIP IP phones in Cisco Unified SIP SRST. • *pool-tag*—Unique number assigned to the pool. Range is 1 to 100. or Enters voice register template configuration mode and defines a template of common parameters for Cisco Unified SIP IP phones. • *template-tag*—Declares a template tag. Range is 1 to 10. or Enters ephone configuration mode. • phone-tag—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones is version and platform-specific. Type ? to display range.
Step 7	**transfer max-length** *max-length* **Example:** `Router(config-register-pool)# transfer max-length 7`	(Optional) Specifies the maximum length of the transfer number. • *max-length*—Maximum length of the transfer number. Range is 3 to 16.
Step 8	**exit** **Example:** `Router(config-register-pool)# exit`	Enters global configuration mode.
Step 9	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode for configuring Cisco Unified CME.
Step 10	**conference transfer-pattern** **Example:** `Router(config-telephony)# conference transfer-pattern`	Enables a Cisco Unified CME system to apply transfer patterns to a conference call using conference softkeys or feature buttons.
Step 11	**end** **Example:** `Router(config-telephony)# end`	Exits telephony-service configuration mode and enters privileged EXEC mode.

Conference Max-Length

Conference calls are allowed when:

- both **conference transfer-pattern** and **transfer-pattern** commands are configured
- dialed digits match the configured transfer pattern

When conference max-length command is configured, the Cisco Unified CME will allow the conferences only if the dialed digits are within the max-length limit.

If configured, the conference max-length command does not impact call transfers.

Note If both **conference max-length** and **transfer max-length** commands are configured, the conference **max-length** command takes precedence for conferences.

Block Trunk-to-Trunk Call Transfers for SIP

To block call transfers to external destinations, perform the following steps.

Restriction Call transfer restrictions apply when transfers are initiated toward external parties, like a PSTN trunk, a SIP trunk, or an H.323 trunk. The restrictions do not apply to transfers to local extensions.

Before You Begin

Cisco Unified CME 9.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **voice register pool** *pool-tag*
   - **voice register template** *template-tag*
4. **transfer-pattern blocked**
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	Enter one of the following commands: • **voice register pool** *pool-tag* • **voice register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters voice register pool configuration mode and creates a pool configuration for a Cisco Unified SIP IP phone in Cisco Unified CME or for a set of Cisco Unified SIP IP phones in Cisco Unified SIP SRST. • *pool-tag*—Unique number assigned to the pool. Range is 1 to 100. Enters voice register template configuration mode and defines a template of common parameters for Cisco Unified SIP IP phones. • *template-tag*—Declares a template tag. Range is 1 to 10.
Step 4	**transfer-pattern blocked** **Example:** `Router(config-register-temp)# transfer-pattern blocked`	Blocks all call transfers for a specific Cisco Unified SIP IP phone or a set of Cisco Unified SIP IP phone.
Step 5	**end** **Example:** `Router(config-register-temp)# end`	Exits voice register template configuration mode and enters privileged EXEC mode.

Enable H.450.12 Capabilities

To enable H.450.12 capabilities globally or by individual dial peer when not all gateway endpoints in your network support H.450.2 and H.450.3 standards, perform the following steps. H.450.12 capabilities are disabled by default to minimize the risk of compatibility issues with other types of H.323 systems. Settings for individual dial peers override the global setting.

Restriction Cisco CME 3.0 and earlier versions do not support H.450.12.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **supplementary-service h450.12** [**advertise-only**]
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **supplementary-service h450.12**
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 service voip** **Example:** `Router(config)# voice service voip`	(Optional) Enters voice service configuration mode to establish global call transfer and forwarding parameters.
Step 4	**supplementary-service h450.12** [**advertise-only**] **Example:** `Router(conf-voi-serv)# supplementary-service h450.12`	(Optional) Enables H.450.12 supplementary services capabilities globally for VoIP endpoints. • This command enables call-by-call detection of H.450 capabilities when some endpoints in your mixed network are H.450-capable and other endpoints are not. This command is disabled by default. • **advertise-only—**(Optional) Advertises H.450 capabilities to the remote end but does not require H.450.12 responses. Use this keyword on Cisco CME 3.1 or later systems if you have a mixed network containing Cisco CME 3.0 systems. This command is also used in dial-peer configuration mode to affect an individual dial peer.
Step 5	**exit** **Example:** `Router(conf-voi-serv)# exit`	(Optional) Exits voice-service configuration mode.

	Command or Action	Purpose
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	(Optional) Enters dial-peer configuration mode.
Step 7	**supplementary-service h450.12** **Example:** `Router(config-dial-peer)# supplementary-service h450.12`	(Optional) Enables H.450.12 supplementary services capabilities for an individual dial peer. This command is disabled by default. This command is also used in voice-service configuration mode to enable H.450.12 services globally. • If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. • If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer. • If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. • If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.
Step 8	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Enable H.323-to-H.323 Connection Capabilities

Vo IP-to-VoIP c onnections permit the termination and reorigination of transferred and forwarded calls over the VoIP network. VoIP-to-VoIP connections are used for hairpin call routing and for H.450 tandem gateways. The only type of VoIP-to-VoIP connection that is supported by Cisco CME 3.1 or a later version is H.323-to-H.323 connection.

VoIP-to-VoIP connections are disabled on the router by default, and they must be explicitly enabled to make use of hairpin call routing or an H.450 tandem gateway. In addition, you must configure a mechanism to direct transferred or forwarded calls to the hairpin or the H.450 tandem gateway, using one of the following methods:

- Enable H.450.12 capabilities globally or on the routes that your transfers and forwards take. See Enable H.450.12 Capabilities, on page 1196.
- Explicitly disable H.450.2 and H.450.3 capabilities globally or on the routes that your transfers and forwards take. See Enable Call Transfer and Forwarding on SCCP Phones at System-Level, on page 1178.

Restriction

- Codecs on all the VoIP dial peers of the H.450 tandem gateway must be the same.
- Only one codec type is supported in the VoIP network at a time, and there are only two codec choices: G.711 (A-law or mu-law) or G.729.
- Transcoding is not supported.
- Codec renegotiation is not supported. For example, if an H.323 call that uses a G.729 codec is received by a Cisco Unified CME system and is forwarded to a voice-mail system that requires a G.711 codec, the codec cannot be renegotiated from G.729 to G.711.
- H.323-to-SIP hairpin call routing is supported only with Cisco Unity Express. For more information, see Integrating Cisco CallManager Express with Cisco Unity Express.
- Cisco Unified Communications Manager must use a media termination point (MTP), intercluster trunk (ICT) mode, and slow start.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections h323 to h323**
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 service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode to establish global call transfer and forwarding parameters.
Step 4	**allow-connections h323 to h323** **Example:** `Router(conf-voi-serv)# allow-connections h323 to h323`	Enables VoIP-to-VoIP call connections. Use the **no** form of the command to disable VoIP-to-VoIP connections; this is the default.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-voi-serv)# end`	Returns to privileged EXEC mode.

Forward Calls Using Local Hairpin Routing

When Cisco Unified CME is used to forward calls that originate on phones that do not support the H.450.3 standard such as Cisco Unified Communications Manager phones, local hairpin routing must be used to forward the calls. For calling parties whose numbers match the pattern specified, the system automatically detects whether H.450.3 is supported and uses the appropriate method to forward calls.

To enable hairpin routing, you must denote the originating and terminating legs of the hairpin. To forward calls to Cisco Unity Express, connections must be allowed to a SIP trunk.

Optionally, you can disable the use of H.450.3 but this is not required because the system automatically detects calls on which H.450.3 is not supported and local hairpin routing is required when the calling-party numbers match the pattern specified.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **call-forward pattern** *pattern*
5. **calling-number local**
6. **exit**
7. **voice service voip**
8. **allow connections** *from-type* **to** *to-type*
9. **supplementary-service h450.3**
10. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**call-forward pattern** *pattern* **Example:** `Router(config-telephony)# call-forward pattern 6000`	Specifies the calling-party numbers for which to allow call forwarding with automatic detection of whether H.450.3 is supported. If H.450.3 is supported, H.450.3 is used for the forward and, if not, local hairpin is used. • *pattern*—Digits to match for call forwarding. A pattern of .T forwards all calling parties.
Step 5	**calling-number local** **Example:** `Router(config-telephony)# calling-number local`	(Optional) Replaces a calling-party number and name with the forwarding-party (local) number and name for hairpin-forwarded calls only. • Before Cisco CME 3.3, this command must be used with Tool Command Language (Tcl) script app-h450-transfer.2.0.0.7 or a later version. The local-hairpin attribute-value (AV) pair must be set to 1.
Step 6	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 7	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode.
Step 8	**allow connections** *from-type* **to** *to-type* **Example:** `Router(conf-voi-serv)# allow connections h323 to sip`	Allows connections between specific types of endpoints in a network. • *from-type*—Originating endpoint type. Valid choices are **h323** and **sip**. • *to-type*—Terminating endpoint type. Valid choices are **h323** and **sip**.
Step 9	**supplementary-service h450.3** **Example:** `Router(conf-voi-serv)# no supplementary-service h450.3`	(Optional) Enables H.450.3 supplementary services capabilities exchange globally. This is the default. Use the **no** form of this command to disable H.450.3 capabilities globally. This command can also be used in dial-peer configuration mode to disable H.450.3 functionality for a single dial peer.

	Command or Action	Purpose
		Note If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.
Step 10	**end** **Example:** `Router(config-voi-serv)# end`	Exits to privileged EXEC mode.

Enable H.450.7 and QSIG Supplementary Services at System-Level

To enable H.4350.7 capabilities and QSIG supplementary services on all dial peers, perform the following steps.

Restriction

- QSIG integration supports SCCP phones only.
- QSIG integration is exclusive; once QSIG integration is configured, QSIG transit node capability is disabled. There is no dial-peer control to enable either transit or originate/terminate capability on a call by call basis.
- If you enable QSIG supplementary services at a system-level, you cannot disable the capability on individual dial peers.

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **supplementary-service h450.7**
5. **qsig decode**
6. **exit**
7. **voice service pots**
8. **supplementary-service qsig call-forward**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode to define global call transfer and forwarding parameters.
Step 4	**supplementary-service h450.7** **Example:** `Router(config-voi-serv)# supplementary-service h450.7`	Enables H.450.7 supplementary services capabilities exchange at a system-level.
Step 5	**qsig decode** **Example:** `Router(config-voi-serv)# qsig decode`	Enables decoding for QSIG supplementary services.
Step 6	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits VoIP voice-service configuration mode.
Step 7	**voice service pots** **Example:** `Router(config)# voice service pots`	Enters POTS voice-service configuration mode to define global call transfer and forwarding parameters.
Step 8	**supplementary-service qsig call-forward** **Example:** `Router(config-voi-serv)# supplementary-service qsig call-forward`	Enables QSIG call-forwarding supplementary services (ISO 13873) to forward calls to another number.
Step 9	**end** **Example:** `Router(config-voi-serv)# end`	Exits to privileged EXEC mode.

Enable H.450.7 and QSIG Supplementary Services on a Dial Peer

To enable H.4350.7 capabilities and QSIG supplementary services on an individual dial peer, perform the following steps.

Restriction

- QSIG integration supports SCCP phones only.
- QSIG integration is exclusive; once QSIG integration is configured, QSIG transit node capability is disabled. There is no dial-peer control to enable either transit or originate/terminate capability on a call by call basis.
- If you enable QSIG supplementary services at a system-level, you cannot enable or disable the capability on individual dial peers.

Before You Begin

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **qsig decode**
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **supplementary-service h450.7**
8. **exit**
9. **dial-peer voice** *tag* **pots**
10. **supplementary-service qsig call-forward**
11. **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.

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode to define global call transfer and forwarding parameters.
Step 4	**qsig decode** **Example:** `Router(config-voi-serv)# qsig decode`	Enables decoding for QSIG supplementary services.
Step 5	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits VoIP voice-service configuration mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	Enters dial-peer configuration mode to define parameters for an individual dial peer.
Step 7	**supplementary-service h450.7** **Example:** `Router(config-dial-peer)# supplementary-service h450.7`	Enables H.450.7 supplementary services capabilities exchange on a single dial peer.
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.
Step 9	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 2 pots`	Enters dial-peer configuration mode to define parameters for an individual dial peer.
Step 10	**supplementary-service qsig call-forward** **Example:** `Router(config-dial-peer)# supplementary-service qsig call-forward`	Enables QSIG call-forwarding supplementary services (ISO 13873) to forward calls to another number.
Step 11	**end** **Example:** `Router(config-dial-peer)# end`	Exits to privileged EXEC mode.

Disable SIP Supplementary Services for Call Forward and Call Transfer

To disable REFER messages for call transfers or redirect responses for call forwarding from being sent to the destination by Cisco Unified CME, perform the following steps. You can disable these supplementary features if the destination gateway does not support them.

Restriction

- In Cisco Unified CME 4.2 and 4.3, when the **supplementary-service sip refer** command is enabled (default) and both the caller being transferred (transferee) and the phone making the transfer (transferor) are SIP, but the transfer-to phone is SCCP, Cisco Unified CME hairpins the call to the transfer-to phone after receiving the REFER request from transferor instead of sending the REFER request to the transferee.

Before You Begin

Cisco Unified CME 4.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **voice service voip**
   - **dial-peer voice** *tag* **voip**
4. **no supplementary-service sip moved-temporarily**
5. **no supplementary-service sip refer**
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	Enter one of the following commands: • **voice service voip** • **dial-peer voice** *tag* **voip**	Enters voice-service configuration mode to set global parameters for VoIP features. or

	Command or Action	Purpose

	Example:
	`Router(config)# voice service voip or`
	`Router(config)# dial-peer voice 99 voip`
		Enters dial peer configuration mode to set parameters for a specific dial peer.

Step 4	**no supplementary-service sip moved-temporarily**
	
	Example:
	`Router(conf-voi-serv)# no supplementary-service sip moved-temporarily`
	`or`
	`Router(config-dial-peer)# no supplementary-service sip moved-temporarily`
		Disables SIP redirect response for call forwarding either globally or for a dial peer.
		
		Sending redirect message to the destination is the default behavior.

Step 5	**no supplementary-service sip refer** **Example:** `Router(conf-voi-serv)# no supplementary-service sip refer or Router(config-dial-peer)# no supplementary-service sip refer`	Disables SIP REFER message for call transfers either globally or for a dial peer. Sending REFER message to the destination is the default behavior.

Step 6	**end**
	
	Example:
	`Router(config-voi-serv)# end or`
	`Router(config-dial-peer)# end`
		Exits to privileged EXEC mode.

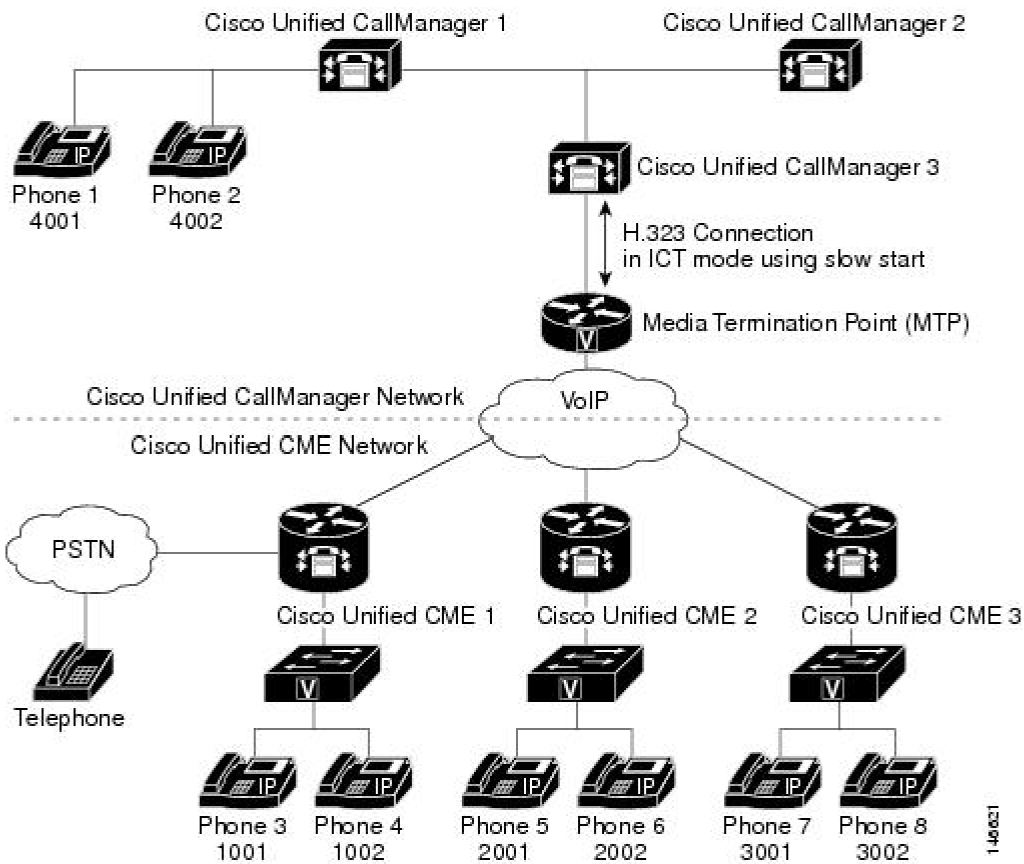
Enable Interworking with Cisco Unified Communications Manager

If Cisco CME 3.1 or later and Cisco Unified Communications Manager are used in the same network, some additional configuration is necessary, as described in the following sections:

- Configure Cisco CME 3.1 or Later to Interwork with Cisco Unified Communications Manager, on page 1208
- Enable Cisco Unified Communications Manager to Interwork with Cisco Unified CME, on page 1212
- Troubleshooting Call Transfer and Forward Configuration, on page 1212

Figure 54: Network with Cisco Unified CME and Cisco Unified Communications Manager, on page 1208 shows a network containing Cisco Unified CME and Cisco Unified Communications Manager systems.

Figure 54: Network with Cisco Unified CME and Cisco Unified Communications Manager



Prerequisites

- Cisco Unified CME must be configured to forward calls using local hairpin routing. For configuration information, see Forward Calls Using Local Hairpin Routing, on page 1200.

Configure Cisco CME 3.1 or Later to Interwork with Cisco Unified Communications Manager

All of the commands in this section are optional because they are set by default to work with Cisco Unified Communications Manager. They are included here only to explain how to implement optional capabilities or return non default settings to their defaults.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **telephony-service ccm-compatible**
6. **h225 h245-address on-connect**
7. **exit**
8. **supplementary-service h225-notify cid-update**
9. **exit**
10. **voice class h323** *tag*
11. **telephony-service ccm-compatible**
12. **h225 h245-address on-connect**
13. **exit**
14. **dial-peer voice** *tag* **voip**
15. **supplementary-service h225-notify cid-update**
16. **voice-class h323** *tag*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode to establish global parameters.
Step 4	**h323** **Example:** `Router(conf-voi-serv)# h323`	Enters H.323 voice-service configuration mode.
Step 5	**telephony-service ccm-compatible** **Example:** `Router(conf-serv-h323)# telephony-service ccm-compatible`	(Optional) Globally enables a Cisco CME 3.1 or later system to detect Cisco Unified Communications Manager and exchange calls with it. This is the default configuration.

	Command or Action	Purpose
		• Use the **no** form of this command to disable Cisco Unified Communications Manager detection and exchange. We do not recommend using the **no** form of the command. • Using this command in an H.323 voice class definition allows you to specify this behavior for an individual dial peer.
Step 6	**h225 h245-address on-connect** **Example:** `Router(conf-serv-h323)# h225 h245-address on-connect`	(Optional) Globally enables a delay for the H.225 message exchange of an H.245 transport address until a call is connected. The delay allows Cisco Unified Communications Manager to generate local ringback for calls to Cisco Unified CME phones. This is the default configuration. • The **no** form of this command disables the delay. We do not recommend using the **no** form of the command. • Using this command in an H.323 voice class definition allows you to specify this behavior for an individual dial peer.
Step 7	**exit** **Example:** `Router(conf-serv-h323)# exit`	Exits H.323 voice-service configuration mode.
Step 8	**supplementary-service h225-notify cid-update** **Example:** `Router(conf-voi-serv)# supplementary-service h225-notify cid-update`	(Optional) Globally enables H.225 messages with caller-ID updates to be sent to Cisco Unified Communications Manager. This is the default configuration. • The **no** form of the command disables caller-ID update. We do not recommend using the **no** form of the command. This command is also used in dial-peer configuration mode to affect a single dial peer. • If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default. • If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer. • If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.
Step 9	**exit** **Example:** `Router(config-voice-service)# exit`	Exits voice-service configuration mode.
Step 10	**voice class h323** *tag* **Example:** `Router(config)# voice class h323 48`	(Optional) Creates a voice class that contains commands to be applied to one or more dial peers.

	Command or Action	Purpose
Step 11	**telephony-service ccm-compatible** **Example:** `Router(config-voice-class)# telephony-service ccm-compatible`	(Optional) Enables the dial peer to exchange calls with a Cisco Unified Communications Manager system when this voice class is applied to a dial peer. This is the default configuration. • The **no** form of the command disables call exchange with Cisco Unified Communications Manager. We do not recommend using the **no** form of the command.
Step 12	**h225 h245-address on-connect** **Example:** `Router(config-voice-class)# h225 h245-address on-connect`	(Optional) Enables the calls that use this dial peer to delay the exchange of H.225 messages that contain the H.245 transport address until calls are connected, when this voice class is applied to a dial peer. The delay allows the playing of local ringback for calls from Cisco Unified Communications Manager. This is the default configuration. • The **no** form of this command disables the delay. We do not recommend using the **no** form of the command.
Step 13	**exit** **Example:** `Router(config-voice-class)# exit`	Exits voice-class configuration mode.
Step 14	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 28 voip`	(Optional) Enters dial-peer configuration mode to set parameters for an individual dial peer.
Step 15	**supplementary-service h225-notify cid-update** **Example:** `Router(config-dial-peer)# no supplementary-service h225-notify cid-update`	(Optional) Enables H.225 messages with caller-ID updates to Cisco Unified Communications Manager for a specific dial peer. This is the default configuration. • The **no** form of the command disables caller-ID updates. We do not recommend using the **no** form of the command.
Step 16	**voice-class h323** *tag* **Example:** `Router(config-dial-peer)# voice-class h323 48`	(Optional) Applies the previously defined voice class with the specified tag number to this dial peer.
Step 17	**end** **Example:** `Router(config-dial-peer)# end`	Exits to privileged EXEC mode.

What to Do Next

Set up Cisco Unified Communications Manager using the configuration procedure in the Enable Cisco Unified Communications Manager to Interwork with Cisco Unified CME, on page 1212.

Enable Cisco Unified Communications Manager to Interwork with Cisco Unified CME

To enable Cisco Unified Communications Manager to interwork with Cisco CME 3.1 or a later version, perform the following steps in addition to the normal Cisco Unified Communications Manager configuration.

Step 1 Set Cisco Unified Communications Manager service parameters. From Cisco Unified Communications Manager Administration, choose Service Parameters. Choose the Cisco Unified Communications Manager service, and make the following settings:

- Set the H323 FastStart Inbound service parameter to False.
- Set the Send H225 User Info Message service parameter to H225 Info for Ring Back.

Step 2 Configure Cisco Unified CME as an ICT in the Cisco Unified Communications Manager network. For information about different intercluster trunk types and configuration instructions, see Cisco Unified Communications Manager documentation.

Step 3 Ensure that the Cisco Unified Communications Manager network uses an MTP. The MTP is required to provide DSP resources for transcoding and for sending and receiving G.729 calls to Cisco Unified CME. All media streams between Cisco Unified Communications Manager and Cisco Unified CME must pass through the MTP because Cisco CME 3.1 does not support transcoding. For more information, see Cisco Unified Communications Manager documentation.

Step 4 Set up dial peers to establish routing using the instructions in the Dial Peer Configuration on Voice Gateway Routers guide.

Troubleshooting Call Transfer and Forward Configuration

Step 1 If you encounter lack of ringback on direct calls from a Cisco Unified Communications Manager phone to an IP phone on a Cisco Unified CME system, check the **show running-config** command output to ensure that the following two commands do *not* appear: **no h225 h245-address on-connect** and **no telephony-service ccm-compatible**. These commands should be enabled, which is their default state.

Step 2 Use the **debug h225 asn1** command to display the H.323 messages that are sent from the Cisco Unified CME system to the Cisco Unified Communications Manager system to see if the H.245 address is being sent too early.

Step 3 For calls that are routed using VoIP-to-VoIP connections, use the **show voip rtp connections detail** command to display the call identification number, IP addresses, and port numbers involved for all VoIP call legs. This command includes VoIP-to-POTS and VoIP-to-VoIP call legs. The following is sample output for this command:

```
Router# show voip rtp connections detail
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP   RmtRTP   LocalIP         RemoteIP
1   7       8          16586      22346   172.27.82.2     172.29.82.2
```

```
2   8       7          17010      16590   172.27.82.2     209.165.202.129

Found 2 active RTP connections
```

Step 4 Use the **show call prompt-mem-usage detail** command to see information on ringback tone generation that uses the interactive voice response (IVR) prompt playback mechanism. This ringback is needed for hairpin transfers that are committed during the alerting-of-the-transfer-destination phase of the call and for calls to destinations that do not provide in-band ringback tone, such as IP phones (FXS analog ports do provide in-band ringback tone). Ringback tone is played to the transferred party by the Cisco Unified CME system that performs the transfer (the system attached to the transferring party). The system automatically generates tone prompts as needed based on the network-locale setting for the Cisco Unified CME system.

If you are not getting ringback tone when you should, use the **show call prompt-mem-usage** command to ensure that the correct prompt is loaded and playing. The following sample output indicates that a prompt is playing ("Number of prompts playing") and indicates the country code used for the prompt (GB for Great Britain) and the codec.

```
Router# show call prompt-mem-usage detail
Prompt memory usage:

 config'd   wait  active  free   mc    total    ms      total
file(s) 0200 0001 -001 00200 00001 00002
memory 02097152 00003000 00000000 02094152 00003000
Prompt load counts: (counters reset 0)
success 0(1st try) 0(2nd try), failure 0
Other mem block usage:
mcDynamic mcReader
gauge 00001 00001
Number of prompts playing: 1
Number of start delays : 0
MCs in the ivr MC sharing table
===============================
Media Content: NoPrompt (0x83C64554)
URL:
cid=0, status=MC_READY size=24184 coding=g711ulaw refCount=0
Media Content: tone://GB_g729_tone_ringback (0x83266EC8)
URL: tone://GB_g729_tone_ringback
```

Configure SIP-to-SIP Phone Call Forwarding

To configure SIP-to-SIP call forwarding using a back-to-back user agent (B2BUA) which allows call forwarding on any dial peer, perform the following steps.

Restriction

- SIP-to-SIP call forwarding is invoked only if that phone is dialed directly. Call forwarding is not invoked when the phone number is called through a sequential, longest-idle, or peer hunt group.
- If call forwarding is configured for a hunt group member, call forward is ignored by the hunt group.
- In Cisco Unified CME 4.1 and later versions, Call Forward All requires SIP phones to be configured with a directory number (using **dn** keyword in **number** command); direct line numbers are not supported.

Before You Begin

- Cisco CME 3.4 or a later version.
- Connections between specific types of endpoints in a Cisco IP-to-IP gateway must be configured by using the **allow-connections** command. For configuration information, see Enable Calls in Your VoIP Network, on page 125.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **call-forward b2bua all** *directory- number*
5. **call-forward b2bua busy** *directory- number*
6. **call-forward b2bua mailbox** *directory- number*
7. **call-forward b2bua night-service** *directory- number*
8. **call-forward b2bua noan** *directory- number* **timeout** *seconds*
9. **call-forward b2bua unreachable** *directory- number*
10. **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 register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.

	Command or Action	Purpose
Step 4	**call-forward b2bua all** *directory- number* **Example:** `Router(config-register-dn)# call-forward b2bua all 5005`	Enables call forwarding for a SIP back-to-back user agent so that all incoming calls will be forwarded to the designated directory-number. • In Cisco CME 3.4 and Cisco Unified CME 4.0, this command is also available in voice register pool configuration mode. The configuration under voice register dn takes precedence over the configuration under voice register pool. • If the **call-forward b2bua all** command is configured in voice register pool configuration mode, it applies to all directory numbers on the phone.
Step 5	**call-forward b2bua busy** *directory- number* **Example:** `Router(config-register-dn)# call-forward b2bua busy 5006`	Enables call forwarding for a SIP back-to-back user agent so that incoming calls to an extension that is busy will be forwarded to the designated directory number. • In Cisco CME 3.4 and Cisco Unified CME 4.0, this command is also available in voice register pool configuration mode. The configuration under voice register dn takes precedence over the configuration under voice register pool.
Step 6	**call-forward b2bua mailbox** *directory- number* **Example:** `Router(config-register-dn)# call-forward b2bua mailbox 5007`	Enables call forwarding for a SIP back-to-back user agent so that incoming calls that have been forwarded to a busy or no-answer extension will be forwarded to the recipient's voice mail. • In Cisco CME 3.4 and Cisco Unified CME 4.0, this command is also available in voice register pool configuration mode. The configuration under voice register dn takes precedence over the configuration under voice register pool.
Step 7	**call-forward b2bua night-service** *directory- number* **Example:** `Router(config-register-dn)# call-forward b2bua night-service 5007`	Enables call forwarding for a SIP back-to-back user agent so that incoming calls that have been forwarded to a busy or no-answer extension will be forwarded to the recipient's voice mail. • In Cisco CME 3.4 and Cisco Unified CME 4.0, this command is also available in voice register pool configuration mode. The configuration under voice register dn takes precedence over the configuration under voice register pool.
Step 8	**call-forward b2bua noan** *directory- number* **timeout** *seconds* **Example:** `Router(config-register-dn)# call-forward b2bua noan 5010 timeout 10 or Router(config-register-pool)# call-forward b2bua noan 5010 timeout 10`	Enables call forwarding for a SIP back-to-back user agent so that incoming calls to an extension that does not answer will be forwarded to the designated directory number. • In Cisco CME 3.4 and Cisco Unified CME 4.0, this command is also available in voice register pool configuration mode. The configuration under voice register dn takes precedence over the configuration under voice register pool.

	Command or Action	Purpose
		• **timeout** *seconds*—Duration that a call can ring before it is forwarded to the destination directory number. Range: 3 to 60000. Default: 20.
Step 9	**call-forward b2bua unreachable** *directory-number* **Example:** `Router(config-register-dn)# call-forward b2bua unreachable 5009 or Router(config-register-pool)# call-forward b2bua unreachable 5009`	(Optional) Enables call forwarding for a SIP back-to-back user agent so that calls can be forwarded to a phone that has not registered in Cisco Unified CME. • Target directory-number must be configured in Cisco Unified CME. • In Cisco CME 3.4 and Cisco Unified CME 4.0, this command is also available in voice register pool configuration mode. The configuration under voice register dn takes precedence over the configuration under voice register pool. • This command was removed in Cisco Unified CME 4.1.
Step 10	**end** **Example:** `Router(config-register-dn)# end`	Exits to privileged EXEC mode.

Configure Call Forward Unregistered for SIP IP Phones

Before You Begin

- Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *tag*
4. **call-forward b2bua unregistered** *directory-number*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register dn** *tag* **Example:** `Router(config)#voice register dn 20`	Enters voice register dn mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.
Step 4	**call-forward b2bua unregistered** *directory-number* **Example:** `Router(config-register-dn)#call-forward b2bua unregistered 2345`	Enables call forwarding for a SIP back-to-back user agent so that all incoming calls are forwarded to the unregistered directory-number.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Troubleshooting Tips for Call Forward Unregistered

- Use the **show dial-peer voice summary** command to check whether a CFU dial peer is created or removed.
- Enable **deb voice reg event**, **deb voice reg state**, and **deb voice reg error** commands to trace the creation and deletion of the CFU dial peer.
- Enable **deb voice reg event**, **deb voip ccapi inout**, **deb voip app callsetup**, **deb voip app core**, **deb voip app state**, and **deb voip app error** commands to trace the call flow for CFU.

Configure Keepalive Timer Expiration in SIP Phones

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **registrar server** [**expires** [**max** *seconds*] [**min** *seconds*]]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(conf)# voice service voip`	Enters voice-service configuration mode and specifies voice-over-IP encapsulation.
Step 4	**sip** **Example:** `Router(conf-serv)# sip`	Enters SIP configuration mode.
Step 5	**registrar server** [**expires** [**max** *seconds*] [**min** *seconds*]] **Example:** `Router(conf-serv-sip)# registrar server expires max 250 min 75`	Enables SIP registrar functionality in Cisco Unified CME. • expires—(Optional) Sets the active time for an incoming registration. • max sec—(Optional) Maximum time for a registration to expire, in seconds. Range: 120 to 86400. • min sec—(Optional) Minimum time for a registration to expire, in seconds.
Step 6	**end** **Example:** `Router (conf-serv-sip)# end`	Returns to privileged EXEC mode.

Configure Call-Forwarding-All Softkey URI on SIP Phones

To specify the uniform resource identifier (URI) for the call forward all (CfwdAll) softkey on supported SIP phones, perform the following steps. This URI and the call forward number is sent to Cisco Unified CME when a user enables Call Forward All on a SIP phone.

Restriction

- This feature is supported only on Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.
- If a user enables Call Forward All using the CfwdAll softkey, it is enabled on the primary line.

Before You Begin

- Cisco Unified CME 4.1 or a later version.
- The **mode cme** command must be enabled in Cisco Unified CME.
- Call Forward All must be enabled on the directory number. For information, see Configure SIP-to-SIP Phone Call Forwarding, on page 1213.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **call-feature-uri cfwdall** *service-uri*
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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set global parameters for all supported SIP phones in a Cisco Unified CME environment.
Step 4	**call-feature-uri cfwdall** *service-uri* **Example:** `Router(config-register-global)# call-feature-uri cfwdall http://1.4.212.11/cfwdall`	Specifies the URI for soft keys on SIP phones connected to a Cisco Unified CME router.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Specify Number of 3XX Responses To be Handled on SIP Phones

To specify how many subsequent 3XX responses an originating SIP phone can handle for a single call when the terminating side is a forwarding party which does not use B2BUA, perform the following steps.

Before You Begin

- Cisco CME 3.4 or a later version.
- The **mode cme** command must be enabled

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **phone-redirect-limit** *number*
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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.

	Command or Action	Purpose
Step 4	**phone-redirect-limit** *number* **Example:** `Router(config-register-global)# phone-redirect-limit 8`	Changes the default number of 3XX responses a SIP phone that originates a call can handle for a single call. • Default: 5
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Configure Call Transfer on SIP Phones

To create and apply a template to enable call transfer softkeys on an individual SIP phone in Cisco Unified CME, perform the following steps.

Restriction

- Blind transfer is not supported on certain phones such as Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, or 7971GE.
- In Cisco Unified CME 4.1, the soft key display can be customized only for certain IP phones, such as Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE. For configuration information, see Modify Softkey Display on SIP Phone, on page 942.

Before You Begin

Cisco CME 3.4 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **transfer-attended**
5. **transfer-blind**
6. **exit**
7. **voice register pool** *pool-tag*
8. **template** *template-tag*
9. **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 register template** *template-tag* **Example:** `Router(config)# voice register template 1`	Enters voice register template configuration mode to define a template of common parameters for SIP phones in Cisco Unified CME. • Range: 1 to 5
Step 4	**transfer-attended** **Example:** `Router(config-register-template)# transfer-attended`	Enable a soft key for attended transfer on any supported SIP phone that uses a template in which this command is configure.
Step 5	**transfer-blind** **Example:** `Router(config-register-template)# transfer-blind`	Enable a soft key for blind transfer on any supported SIP phone that uses a template in which this command is configure.
Step 6	**exit** **Example:** `Router(config-register-template)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 7	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for SIP phones.
Step 8	**template** *template-tag* **Example:** `Router(config-register-pool)#` **voice register pool 1**	Applies a template created with the **voice register template** command. • *template-tag*—Range: 1 to 5
Step 9	**end** **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.

Configuration Examples for Call Transfer and Forwarding

Example for Configuring H.450.2 and H.450.3 Support

The following example sets all transfers and forwards that are initiated by a Cisco CME 3.0 or later system to use the H.450 standards, globally enables H.450.2 and H.450.3 capabilities, and disables those capabilities for dial peer 37. The **supplementary-service** commands under voice-service configuration mode are not necessary because these values are the default, but they are shown here for illustration.

```
telephony-service
transfer-system full-consult
transfer-pattern .T
call-forward pattern .T
!
voice service voip
supplementary-service h450.2

supplementary-service h450.3

!
dial-peer voice 37 voip
destination-pattern 555....
session target ipv4:10.5.6.7

no supplementary-service h450.2

no supplementary-service h450.3
```

Example for Configuring Basic Call Forwarding

The following example sets up forwarding for extension 2777 to extension 2513 on all calls, busy, and no answer. During night service hours, calls are forwarded to a different number, extension 2879.

```
ephone-dn 20
 number 2777
 call-forward all 2513

 call-forward busy 2513

 call-forward noan 2513 timeout 45
 call-forward night-service 2879
```

Example for Configuring Call Forwarding Blocked for Local Calls

In the following example, extension 2555 is configured to not forward local calls that are internal to the Cisco Unified CME system. Extension 2222 dials extension 2555. If 2555 is busy, the caller hears a busy tone. If 2555 does not answer, the caller hears ringback. The internal call is not forwarded.

```
ephone-dn 25
 number 2555
 no forward local-calls
 call-forward busy 2244
 call-forward noan 2244 timeout 45
```

Example for Configuring Transfer Patterns

The following example shows how to configure transfer patterns beginning with 1234:

```
Router# configure terminal
Router(config)# telephony-service
Router(config-telephony)# transfer-pattern 1234
```

Example for Configuring Maximum Length of Transfer Number

The following example shows how to configure the maximum length of the transfer number under voice register pool 1. Because the maximum length is configured as 5, only call transfers to Cisco Unified SIP IP phones with a five-digit directory number are allowed. All call transfers to directory numbers with more than five digits are blocked.

```
Router# configure terminal
Router(config)# voice register pool 1
Router(config-register-pool)# transfer max-length 5
```

The following example shows how to configure the maximum length of the transfer number for a set of phones under voice register template 2:

```
Router# configure terminal
Router(config)# voice register template 2
Router(config-register-temp)# transfer max-length 10
```

Example for Configuring Conference Transfer Patterns

The following example configures transfer patterns that allow conference calls:

```
Router# configure terminal
Router(config)# telephony-service
Router(config-telephony)# transfer-pattern 1357
Router(config-telephony)# transfer-pattern 222....
Router(config-telephony)# conference transfer-pattern
```

Example for Blocking All Call Transfers

The following example shows how to block all call transfers for voice register pool 5:

```
Router(config)# voice register pool 5
Router(config-register-pool)# transfer-pattern ?
blocked  global transfer pattern not allowed
Router(config-register-pool)# transfer-pattern blocked
```

The following example shows how to block all call transfers for a set of Cisco Unified SIP IP phones defined by voice register template 9:

```
Router(config)# voice register template 9
Router(config-register-temp)# transfer-pattern ?
blocked  global transfer pattern not allowed
Router(config-register-temp)# transfer-pattern blocked
```

Example for Configuring Selective Call Forwarding

The following example sets call forwarding on busy and no answer for ephone-dn 38 only for its primary number, 2777. Callers who dial 2778 will hear a busy signal if the ephone-dn is busy or ringback if there is no answer.

```
ephone-dn 38
number 2777 secondary 2778
call-forward busy 3000 primary
call-forward noan 3000 primary timeout 45
```

Example for Configuring Call Transfer

The following example limits transfers from ephone 6, extension 2977, to numbers containing a maximum of 8 digits.

```
telephony-service
load 7910 P00403020214
load 7960-7940 P00305000600
load 7914 S00103020002
load 7905 CP7905040000SCCP040701A
load 7912 CP7912040000SCCP040701A
max-ephones 100
max-dn 500
ip source-address 10.104.8.205 port 2000
max-redirect 20
system message XYZ Inc.
create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
voicemail 7189
max-conferences 8 gain -6
moh music-on-hold.au
web admin system name admin1 password admin1
dn-webedit

time-webedit

transfer-system full-consult
transfer-pattern 91..........
transfer-pattern 92......
transfer-pattern 93......
transfer-pattern 94......
transfer-pattern 95......
transfer-pattern 96......
transfer-pattern 97......
transfer-pattern 98......
transfer-pattern 99......
secondary-dialtone 9
fac standard
ephone-template 2
transfer max-length 8
ephone-dn 4
number 2977
ephone 6
button 1:4
ephone-template 2
```

Example for Configuring Call Transfer Recall for SCCP Phones

The following example shows that transfer recall is enabled globally. After 60 seconds an unanswered call is forwarded back to the phone that initiated the transfer (transferor).

```
telephony-service
 max-ephones 100
 max-dn 240
 timeouts transfer-recall 60
 max-conferences 8 gain -6
 transfer-system full-consult
```

The following example shows that transfer recall is enabled for extension 1030 (ephone-dn 103), which is assigned to ephone 3. If extension 1030 forwards a call and the transfer-to party does not answer, after 60 seconds the unanswered call is sent back to extension 1030 (transferor). The **timeouts transfer-recall** command can also be set in an ephone-dn template and applied to one or more directory numbers.

```
ephone-dn  103
number 1030
name Smith, John
timeouts transfer-recall 60
!
ephone  3
mac-address 002D.264E.54FA
type 7962
button  1:103
```

Example for Configuring Call-Transfer Recall for SIP Phones

The following example shows that transfer recall is enabled globally. After 20 seconds, an unanswered call is forwarded back to the phone that initiated the transfer (transferor).

```
voice register global
 mode cme
 source-address 8.39.17.29 port 5060
 timeouts transfer-recall 20
 max-dn 100
 max-pool 100
 tftp-path flash:
 create profile sync 0342574150542703
 keepalive 140
 auto-register
```

The following example shows that transfer recall is enabled for extension 111 (voice register dn 1). If extension 111 forwards a call to voice register dn 2 and the transfer-to party does not answer, after 20 seconds the unanswered call is sent back to extension 1111 (transferor).

```
voice register dn  1
 timeouts transfer-recall 20
 number 111
voice register dn  2
 number 222
```

Example for Enabling H.450.12 Capabilities

The following example globally disables H.450.12 capabilities and then enables them only on dial peer 24.

```
voice service voip
no supplementary-service h450.12
!
dial-peer voice 24 voip
destination-pattern 555....
session target ipv4:10.5.6.7

supplementary-service h450.12
```

Example for Enabling H.450.7 and QSIG Supplementary Services

The following example implements QSIG supplementary services on extension 74367 and globally enables H.450.7 supplementary services and QSIG call-forwarding supplementary services.

```
telephony-service
voicemail 74398
transfer-system full-consult
ephone-dn 25
number 74367
mwi qsig
call-forward all 74000
voice service voip
supplementary-service h450.7
voice service pots
supplementary-service qsig call-forward
```

Example for Configuring Cisco Unified CME and Cisco Unified Communications Manager in Same Network

The following example shows a running configuration for a Cisco CME 3.1 or later router that has a Cisco Unified Communications Manager in its network.

```
Router# show running-config

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
enable password pswd
!
aaa new-model
!
!
aaa session-id common
no ip subnet-zero
!
ip dhcp pool phone1
 host 172.24.82.3 255.255.255.0
 client-identifier 0100.07eb.4629.9e
 default-router 172.24.82.2
 option 150 ip 172.24.82.2
!
ip dhcp pool phone2
 host 172.24.82.4 255.255.255.0
 client-identifier 0100.0b5f.f932.58
 default-router 172.24.82.2
 option 150 ip 172.24.82.2
!
ip cef
no ip domain lookup
no mpls ldp logging neighbor-changes
no ftp-server write-enable
!
voice service voip
 allow-connections h323 to h323
!
voice class codec 1
 codec preference 1 g711ulaw
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
 ip address 172.24.82.2 255.255.255.0
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 172.24.82.2
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.24.82.1
ip route 192.168.254.254 255.255.255.255 172.24.82.1
!
ip http server
!
tftp-server flash:P00303020700.bin
!
voice-port 1/0/0
!
voice-port 1/0/1
!
```

```
dial-peer cor custom
!
dial-peer voice 1001 voip
 description points-to-CCM
 destination-pattern 1.T
 voice-class codec 1
 session target ipv4:172.26.82.10
!
dial-peer voice 1002 voip
 description points to router
 destination-pattern 4...
 voice-class codec 1
 session target ipv4:172.25.82.2
!
dial-peer voice 1 pots
 destination-pattern 3000
 port 1/0/0
!
dial-peer voice 1003 voip
 destination-pattern 26..
 session target ipv4:10.22.22.38
!
!
telephony-service
 load 7960-7940 P00303020700
 max-ephones 48
 max-dn 15
 ip source-address 172.24.82.2 port 2000
 create cnf-files version-stamp Jan 01 2002 00:00:00
 keepalive 10
 max-conferences 4
 moh minuet.au
 transfer-system full-consult
 transfer-pattern ....
!
ephone-dn  1
 number 3001
 name abcde-1
 call-forward busy 4001
!
ephone-dn  2
 number 3002
 name abcde-2
!
ephone-dn  3
 number 3003
 name abcde-3
!
ephone-dn  4
 number 3004
 name abcde-4
!
ephone  1
 mac-address 0003.EB27.289E
 button  1:1 2:2
!
ephone  2
 mac-address 000D.39F9.3A58
 button  1:3 2:4
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 password pswd
!
end
```

Example for Configuring H.450 Tandem Gateway Working with Cisco Unified CME and Cisco Unified Communications Manager

The following example shows a sample configuration for a Cisco CME 3.1 or later system that is linked to an H.450 tandem gateway that serves as a proxy for Cisco Unified Communications Manager.

```
Router# show running-config

Building configuration...

Current configuration : 1938 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password pswd
!
aaa new-model
!
aaa session-id common
no ip subnet-zero
!
ip cef
no ip domain lookup
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
voice call send-alert
!
voice service voip
```

```
 allow-connections h323 to h323
 supplementary-service h450.12
 h323
!
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
codec preference 3 g729br8
!
interface FastEthernet0/0
ip address 172.27.82.2 255.255.255.0
duplex auto
speed auto
h323-gateway voip interface
h323-gateway voip h323-id host24
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.26.82.1
ip route 0.0.0.0 0.0.0.0 172.27.82.1
ip http server
!
dial-peer cor custom
!
dial-peer voice 1001 voip
description points-to-CCM
 destination-pattern 4...
session target ipv4:172.24.89.150
!
dial-peer voice 1002 voip
description points to CCME1
destination-pattern 28..
session target ipv4:172.24.22.38
!
dial-peer voice 1003 voip
description points to CCME3
destination-pattern 9...
 session target ipv4:192.168.1.29
!
dial-peer voice 1004 voip
description points to CCME2
destination-pattern 29..
session target ipv4:172.24.22.42
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
password pswd
!
end
```

Example for Configuring Call Forward to Cisco Unity Express

The following example enables the ability to forward calls that originate from Cisco Unified Communications Manager phones and are routed through a Cisco Unified CME system to a Cisco Unity Express extension. Call forwarding is enabled for all calling parties, H.450.3 is disabled, and connections are allowed to SIP endpoints.

```
telephony-service
 call-forward pattern .T

voice service voip
 no supplementary-service h450.3
 allow connections from h323 to sip
```

Example for Configuring Call Forward Unregistered for SIP IP Phones

The following example shows CFU configured for voice register dn 20:

```
!
!
!
voice service voip
 allow-connections sip to sip
 sip
  registrar server expires max 250 min 75
!
!
voice register global
 mode cme
 source-address 10.100.109.10 port 5060
 bandwidth video tias-modifier 256 negotiate end-to-end
 max-dn 200
 max-pool 42
 url directory http://1.4.212.11/localdirectory
 create profile sync 0004625832149157
!
voice register dn  20
 number 10
 call-forward b2bua unregistered 2345
!
voice register pool  1
 number 1 dn 20
 id mac 1111.1111.1111
 camera
 video
!
voice register pool  2
id mac 0009.A3D4.1234
```

Example for Configuring Keepalive Timer Expiration in SIP Phones

The following example shows the minimum and maximum registrar server expiration time for SIP phones:

```
Router#show run
!
!
!
!
!
!
voice service voip
allow-connections sip to sip
sip
registrar server expires max 250 min 75
!
!
voice register global
mode cme
source-address 10.100.109.10 port 5060
bandwidth video tias-modifier 256 negotiate end-to-end
max-dn 200
```

Where to Go Next

If you are finished modifying the configuration, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Softkeys

To block the function of the call-forward-all or transfer softkey without removing the key display or to remove the softkey from one or more phones, see Customize Softkeys, on page 925.

Feature Access Codes (FACs)

Phone users can activate and deactivate a phone's call-forward-all setting by using a feature access code (FAC) instead of a soft key on the phone if standard or custom FACs have been enabled for your system. The following are the standard FACs for call forward all:

- **callfwd all**—Call forward all calls. Standard FAC is **1 plus an optional target extension.
- **callfwd cancel**—Cancel call forward all calls. Standard FAC is **2.

For more information about FACs, see Feature Access Codes, on page 757.

Night Service

Calls can be automatically forwarded during night service hours, but you must define the night-service periods, which are the dates or days and hours during which night service will be active. For instance, you may want to designate night service periods that include every weeknight between 5 p.m. and 8 a.m. and all day every Saturday and Sunday. For more information, see Configure Call Coverage Features, on page 1278.

Feature Information for Call Transfer and Forwarding

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

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

Table 101: Feature Information for Call Transfer and Forwarding

Feature Name	Cisco Unified CME Version	Feature Information
Calling Number Local	12.0	Introduced support to configure Calling Number Local feature for Voice Register DNs.
Call Transfer Recall on SIP Phones	11.6	Call Transfer Recall feature returns a transferred call to the phone that initiated the transfer if the destination is busy or does not answer.
Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones	9.5	Introduced support Trunk-to-Trunk Transfer Blocking for Toll Fraud Prevention on Cisco Unified SIP IP Phones.

Feature Name	Cisco Unified CME Version	Feature Information
Call Forwarding	4.1	• Call Forward All synchronization between Cisco Unified CME and SIP phones was added. • Disabling SIP supplementary services for call forward and call transfer was added.
	4.0	• Automatic call forwarding during night service was introduced. • Selective call forwarding was introduced. • Forwarding of local (internal) calls can be blocked. • H.450.7 standards support and QSIG supplementary services capability was introduced.
	3.4	Calls into a SIP device can be forwarded to other SIP or SCCP devices including Cisco Unity, third- party voice mail systems, or an auto-attendant (AA) or other interactive voice response (IVR) devices. SCCP devices may also be forwarded to SIP devices.
	3.1	• Number of digits that can be entered using the CfwdALL (call-forward all) soft key can be limited. • H.450.12 standards support, which provide dynamic detection of H.450.2 and H.450.3 capabilities on a call-by-call basis, was introduced.
	3.0	

Feature Name	Cisco Unified CME Version	Feature Information
		• CFwdALL soft key was introduced. • Local hairpin call routing was supported as an option for networks that cannot support H.450 call transfer and forwarding. This feature requires installation of the Tcl script app_h450_transfer.2.0.0.8.tcl or a later version.
	2.1	Call forwarding using the H.450.3 standard was introduced.
	1.0	Call forwarding for all calls, busy conditions, and no-answer conditions was introduced, using a Cisco-proprietary method.
Call Forward Unregistered	8.6	The Call Forward Unregistered (CFU) feature was introduced for SIP phones.

Feature Name	Cisco Unified CME Version	Feature Information
Call Transfer	4.3	• Call-Transfer Recall was added. • Consultative Call Transfer digit-collection process was modified.
	4.1	• Disabling SIP supplementary services for call transfer and call forward was added.
	4.0	• Default for the **transfer-system** command was changed from the **blind** keyword to the **full-consult** keyword. • Transfers to phones outside the Cisco Unified CME system can be blocked for individual ephones. • Number of digits in transfer destination numbers can be limited.
	3.4	Support for attended and blind transfer s using SIP IP phone directly connected to Cisco CME.
	3.2	• Consultative transfer to monitored lines using direct station select was introduced. • Transcoding between G.711 and G.729 is supported when one leg of a Voice over IP (VoIP)-to-VoIP hairpin call uses G.711 and the other leg uses G.729.
	3.1	

Feature Name	Cisco Unified CME Version	Feature Information
		Support was introduced for the following: • Enhancements for VoIP networks which contain a mix of platforms that support H.450.2 and H.450.3 standards, such as Cisco CME 3.1, Cisco CME 3.0, Cisco ITS V2.1, and platforms that do not support H.450.2 and H.450.3 standards, such as Cisco Unified Communications Manager, Cisco BTS Softswitch (BTS), and Cisco PSTN Gateway (PGW). • H.450.12 standards, which provide dynamic detection of H.450.2 and H.450.3 capabilities on a call-by-call basis. • Automatic detection of Cisco Unified Communications Manager endpoints. • Hairpin VoIP-to-VoIP call routing and routing to an H.450 tandem gateway. • Hairpin call routing does not require a Tcl script.
	3.0	Local hairpin call routing was supported as an option for networks that cannot support H.450 call transfer and forwarding. This feature requires installation of the Tcl script app_h450_transfer.2.0.0.8.tcl or a later version.
	2.1	Consultative transfer using the ITU-T H.450.2 standard was introduced.
	1.0	Call transfer was introduced, using a Cisco proprietary method.

CHAPTER 44

Call Coverage Features

Information About Call Coverage Features

Call Coverage Summary

Call coverage features are used to ensure that all incoming calls to Cisco Unified CME are answered by someone, regardless of whether the called number is busy or does not answer.

Some single-dialed-number call coverage features, such as hunt groups, can send incoming calls to a single extension to a pool of phone agents, while other features, such as call hunt, call waiting, and call forwarding increase the chance of a call being answered by giving it another chance for a connection if the dialed number is not available.

Multiple-dialed-number call coverage features, such as call pickup, night service, and overlaid directory numbers, provide different ways for one person to answer incoming calls to multiple numbers.

Any of the call coverage features can be combined with other call coverage features and with shared lines and secondary numbers to design the call coverage plan that is best suited to your needs.

Table 102: Call Coverage Feature Summary, on page 1240 summarizes call coverage features.

Table 102: Call Coverage Feature Summary

Feature	Description	Example	How Configured
Call Forwarding	Calls are automatically diverted to a designated number on busy, no answer, all calls, or only during night-service hours.	Extension 3444 is configured to send calls to extension 3555 when it is busy or does not answer.	Enable Call Forwarding for a Directory Number, on page 1185 or Configure SIP-to-SIP Phone Call Forwarding, on page 1213
Call Hunt	System automatically searches for an available directory number from a matching group of directory numbers until the call is answered or the hunt is stopped.	Three ephone-dns have the same extension number, 755. One is on the manager's phone and the others are on the assistants' phones. Preference and huntstop are used to make sure that calls always come to the manager's phone first but if they can't be answered, they will ring on the first assistant's phone and if not answered, on the second assistant's phone.	Configure Call Hunt on SCCP Phones, on page 1278 or Configure Call Hunt on SIP Phones, on page 1281
Call Pickup	Calls to unstaffed phones can be answered by other phone users using a soft key or by dialing a short code.	Extension 201 and 202 are both in pickup group 22. A call is received by 201, but no one is there to answer. The agent at 202 presses the GPickUp soft key to answer the call.	Enable Call Pickup, on page 1282
Call Waiting	Calls to busy numbers are presented to phone users, giving them the option to answer them or let them be forwarded.	Extension 564 is in conversation when a call-waiting beep is heard. The phone display shows the call is from extension 568 and the phone user decides to let the call go to voice mail.	Configure Call-Waiting Indicator Tone on SCCP Phone, on page 1285 or Enable Call Waiting on SIP Phones, on page 1290

Feature	Description	Example	How Configured
Cisco CME B-ACD	Calls to a pilot number are automatically answered by an interactive application that presents callers with a menu of choices before sending them to a queue for a hunt group.	The DID number 555-0125 is the pilot number for the XYZ Company. Incoming calls to this pilot number hear a menu of choices; they can press 1 for sales, 2 for service, or 3 to leave a message. The call is forwarded appropriately when callers make a choice.	See Cisco Unified CME B-ACD and Tcl Call-Handling Applications.
Hunt Groups	Calls are forwarded through a pool of agents until answered or sent to a final number.	Extension 200 is a pilot number for the sales department. Extensions 213, 214, and 215 belong to sales agents in the hunt group. When a call to extension 200 is received, it proceeds through the list of agents until one answers. If all the agents are busy or do not answer, the call is sent to voice mail.	Configure Ephone-Hunt Groups on SCCP Phones, on page 1291 or Configure Voice-Hunt Groups, on page 1301
Night Service	Calls to ephone-dns and voice register dns that are not staffed during certain hours can be answered by other phones using call pickup.	Extension 7544 is the cashier's desk but the cashier only works until 3 p.m. A call is received at 4:30 p.m. and the service manager's phone is notified. The service manager uses call pickup to answer the call.	Configure Night Service on SCCP Phones, on page 1315 Configure Night Service on SIP Phones, on page 1318
Overlaid Ephone-dns	Calls to several numbers can be answered by a single agent or multiple agents.	Extensions 451, 452, and 453 all appear on button 1 of a phone. A call to any of these numbers can be answered from button 1.	Configure Overlaid Ephone-dns on SCCP Phones, on page 1326.

Out-of- Dialog REFER

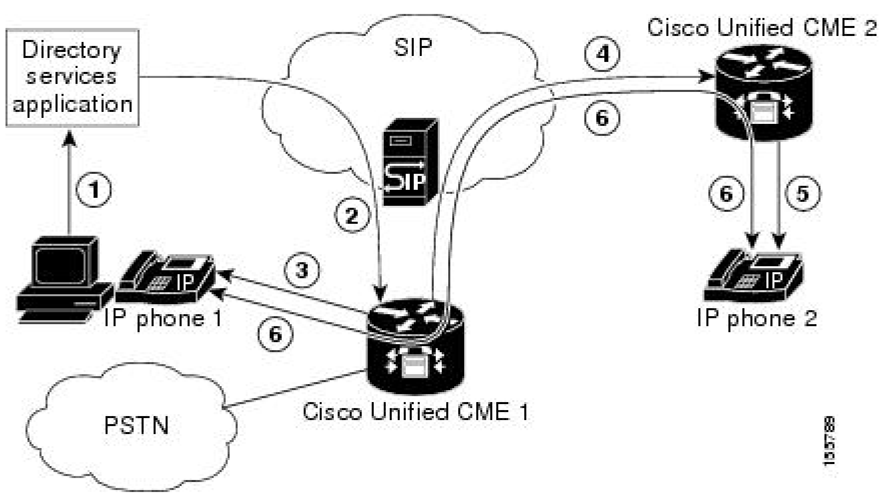
Out-of-dialog REFER (OOD-R) allows remote applications to establish calls by sending a REFER message to Cisco Unified CME without an initial INVITE. After the REFER is sent, the remainder of the call setup is independent of the application and the media stream does not flow through the application. The application using OOD-R triggers a call setup request that specifies the Referee address in the Request-URI and the Refer-Target in the Refer-To header. The SIP messaging used to communicate with Cisco Unified CME is independent of the end-user device protocol which can be SIP, SCCP, H.323, or POTS. Click-to-dial is an example of an application that can be created using OOD-R.

A click-to-dial application allows users to combine multiple steps into one click for a call setup. For example, a user can click a web-based directory application from their PC to look up a telephone number, off-hook their desktop phone, and dial the called number. The application initiates the call setup without the user having to out-dial from their own phone. The directory application sends a REFER message to Cisco Unified CME which sets up the call between both parties based on this REFER.

Figure 55: Click-to-Dial Application using Out-of-Dialog REFER, on page 1242 shows an example of OOD-R being used by a click-to-dial application. In this scenario, the following events occur (refer to the event numbers in the illustration):

1. Remote user clicks to dial.
2. Application sends out-of-dialog REFER to Cisco Unified CME 1.
3. Cisco Unified CME 1 connects to SIP phone 1 (Referee).
4. Cisco Unified CME 1 sends INVITE to Cisco Unified CME 2.
5. Cisco Unified CME 2 sends INVITE to SIP phone 2 (Refer-Target) and the call is accepted.
6. Voice path is created between the two SIP phones.

Figure 55: Click-to-Dial Application using Out-of-Dialog REFER



The initial OOD-R request can be authenticated and authorized using RFC 2617-based digest authentication. To support authentication, Cisco Unified CME retrieves the credential information from a text file stored in flash. This mechanism is used by Cisco Unified CME in addition to phone-based credentials. The same credential file can be shared by other services that require request-based authentication and authorization such as presence service. Up to five credential files can be configured and loaded into the system. The contents of these five files are mutually exclusive, meaning the username and password pairs must be unique across all the files. The username and password pairs must also be different than those configured for SCCP or SIP phones in a Cisco Unified CME system.

For configuration information, see Enable Out-Of-Dialog REFER, on page 1330.

Call Hunt

Call hunt allows you to use multiple directory numbers to provide coverage for a single called number. You do this by assigning the same number to several primary or secondary ephone-dns or by using wildcards in the number associated with the directory numbers.

Calls are routed based on a match between the number dialed and the destination patterns that are associated with dial peers. Through the use of wildcards in destination patterns, multiple dial peers can match a particular called number. Call hunt is the ability to search through the dial peers that match the called number until the call is answered. Call hunt uses a technique called preference to control the order in which dial peers are matched to an incoming call and a technique called huntstop to determine when the search for another matching peer ends.

In Cisco Unified CME, incoming calls search through the virtual dial peers that are automatically created when you define directory numbers. These virtual dial peers are not directly configurable; you must configure the directory number to control call hunt for virtual dial peers.

Channel huntstop is used to stop the search for the two channels of a dual-line directory number. Channel huntstop keeps incoming calls from hunting to the second channel if the first channel is busy or does not answer. This keeps the second channel free for call transfer, call waiting, or three-way conferencing.

Huntstop prevents hunt-on-busy from redirecting a call from a busy phone into a dial peer that has been setup with a catch-all default destination.

For configuration information, see Configure Call Hunt on SCCP Phones, on page 1278 or Configure Call Hunt on SIP Phones, on page 1281.

Call Pickup

Call Pickup allows a phone user to answer a call that is ringing on another phone. Cisco Unified CME 7.1 introduces Call Pickup features for SIP phones. SCCP phones support three types of Call Pickup:

- Directed Call Pickup—Call pickup, explicit ringing extension. Any local phone user can pick up a ringing call on another phone by pressing a soft key and then dialing the extension. A phone user does not need to belong to a pickup group to use this method. The soft key that the user presses, either GPickUp or PickUp, depends on your configuration.
- Group Pickup, Different Group—Call pickup, explicit group ringing extension. A phone user can answer a ringing phone in any pickup group by pressing the GPickUp soft key and then dialing the pickup group number. If there is only one pickup group defined in the Cisco Unified CME system, the phone user can pick up the call simply by pressing the GPickUp soft key. A phone user does not need to belong to a pickup group to use this method.
- Local Group Pickup—Call pickup, local group ringing extension. A phone user can pick up a ringing call on another phone by pressing a soft key and then the asterisk (*) if both phones are in the same

pickup group. The soft key that the user presses, either GPickUp or PickUp, depends on your configuration.

Note SIP phones only support local pickup and group pickup. Directed call pickup is not supported.

The specific soft keys used to access different Call Pickup features on SCCP and SIP phones depends on the configuration in Cisco Unified CME. See the **service directed-pickup** command in Cisco Unified CME Command Reference for a description.

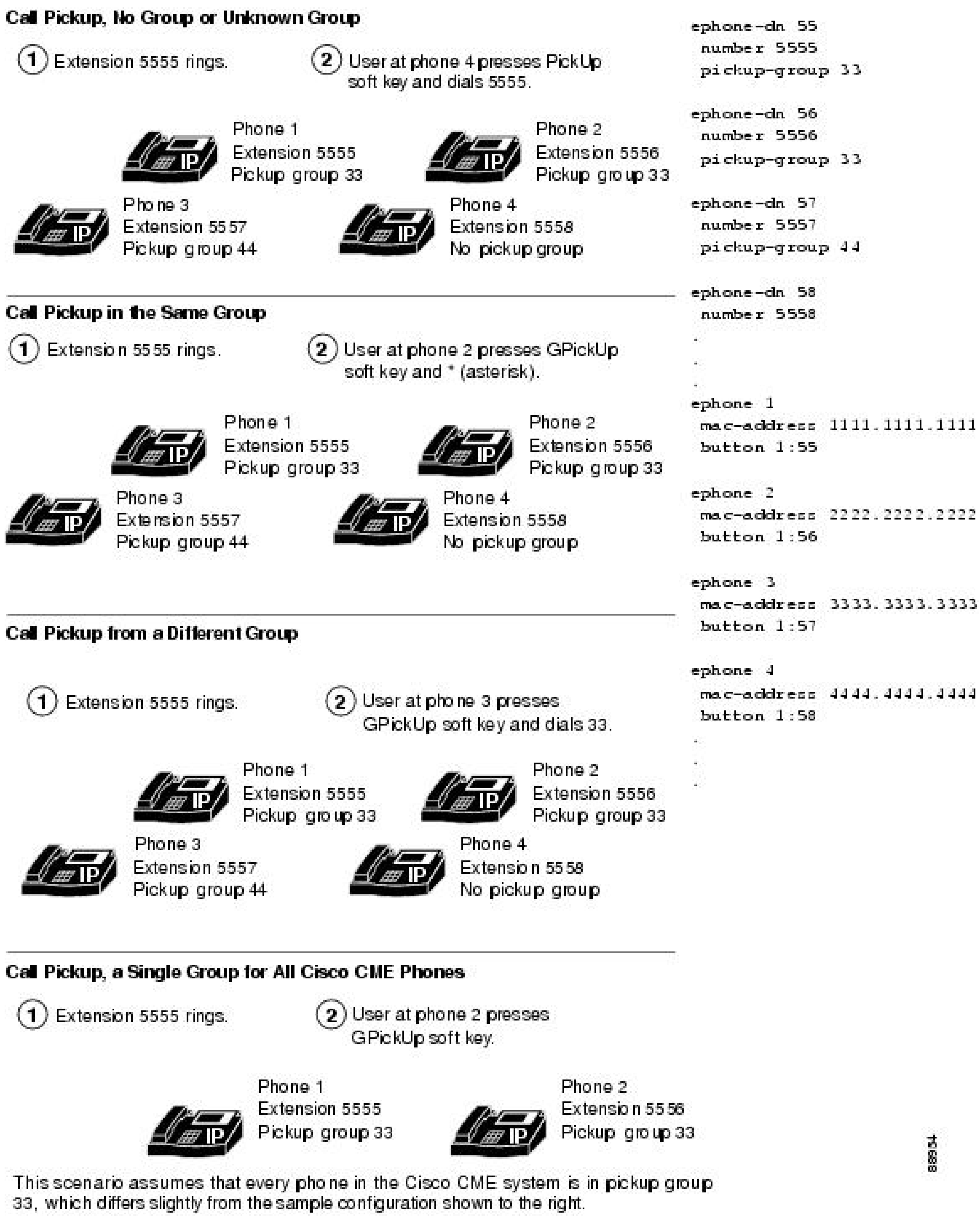
You can assign each directory number to only one pickup group and a directory number must have a pickup group configured to use Local Group Pickup. There is no limit to the number of directory numbers that can be assigned to a single pickup group, or to the number of pickup groups that can be defined in a Cisco Unified CME system.

If more than one call is ringing on the same number, the calls are picked up in the order in which they were received; the call that has been ringing the longest is the first call picked up from that extension number. Remote call pickup is not supported.

Call Pickup features are enabled globally for all phones through Cisco Unified CME. The PickUp and GpickUp soft keys display on supported SCCP and SIP phones by default and can be modified by using a phone template. For configuration information, see Enable Call Pickup, on page 1282.

Figure 56: Call Pickup, on page 1245 shows four call-pickup scenarios.

Figure 56: Call Pickup



Call Waiting

Call waiting allows phone users to be alerted when they receive an incoming call while they are on another call. Phone users hear a call-waiting tone when another party is trying to reach them and, on IP phones, see the calling party information on the phone screen.

Call-waiting calls to IP phones with soft keys can be answered using the Answer soft key. Call-waiting calls to analog phones controlled by Cisco Unified CME systems are answered using hookflash. When phone users answer a call-waiting call, their original call is automatically put on hold. If a phone user does not respond to a call-waiting notification, the call is forwarded as specified in the **call-forward noan** command for that extension.

For an IP phone running SCCP, call waiting for single-line ephone-dns requires two ephone-dns to handle the two calls. Call waiting on a dual-line ephone-dn requires only one ephone-dn because the two channels of the ephone-dn handle the two calls. The audible call-waiting indicator can be either a call-waiting beep or a call-waiting ring. For configuration information, see Configure Call-Waiting Indicator Tone on SCCP Phone, on page 1285.

For a SIP phone, call waiting is automatically enabled when you configure a voice register pool. For SIP phones directly connected to Cisco Unified CME, call waiting can be disabled at the phone-level. For configuration information, see Enable Call Waiting on SIP Phones, on page 1290.

For information on call waiting using Overlaid ephone-dns, see Overlaid Ephone-dns, on page 1274.

Call-Waiting Beep for SCCP Phones

Call-waiting beeps are enabled by default. You can disable the call-waiting beeps that are generated from and accepted by directory numbers. If beep generation is disabled, incoming calls to the directory number do not generate call-waiting beeps. If beep acceptance is disabled, the phone user does not hear beeps when using the directory number for an active call.

Table 103: Call-Waiting Beep Behavior , on page 1246 shows the possible beep behaviors of one ephone-dn calling another ephone-dn that is connected to another caller.

Table 103: Call-Waiting Beep Behavior

Ephone-dn 1 Configuration	Ephone-dn 2 Configuration	Active Call on DN	Incoming Call on DN	Expected Behavior
—	`no call-waiting beep`	DN 1	DN 2	No beep
`no call-waiting beep`	—	DN 1	DN 2	No beep

Ephone-dn 1 Configuration	Ephone-dn 2 Configuration	Active Call on DN	Incoming Call on DN	Expected Behavior
—	`no call-waiting beep generate`	DN 1	DN 2	No beep
—	`no call-waiting beep accept`	DN 1	DN 2	Beep
—	`no call-waiting beep acceptno call-waiting beep generate`	DN 1	DN 2	No beep
`no call-waiting beep`	—	DN 1	DN 1	No beep
`no call-waiting beep generate`	—	DN 1	DN 1	No beep
`no call-waiting beep accept`	—	DN 1	DN 1	No beep
`no call-waiting beep accept no call-waiting beep generate`	—	DN 1	DN 1	No beep
`no call-waiting beep generate`	—	DN 1	DN 2	Beep
`no call-waiting beep accept`	—	DN 1	DN 2	No beep
—	`no call-waiting beep`	DN 1	DN 1	Beep

Call-Waiting Ring for SCCP Phones

Instead of the standard call-waiting beep sound through the handset, you can use a short ring for call-waiting notification. The default is for directory numbers to accept call interruptions, such as call waiting, and to issue a beeping sound for notification.

To use a ring sound, the directory number must accept call-waiting indicator tones. For configuration information, see Configure Call-Waiting Indicator Tone on SCCP Phone, on page 1285 or Enable Call Waiting on SIP Phones, on page 1290.

Cancel Call Waiting

Cancel Call Waiting (CCW) enables an SCCP phone user to disable Call Waiting for a call they originate. The user activates CCW, and thereby disables call waiting, by pressing the cancel call waiting (CW Off) soft key or by dialing the feature access code (FAC) before placing a call. Call Waiting is inactive during that call; anyone calling the user receives normal busy treatment and no call waiting tone interrupts the user's active call. CCW automatically deactivates when the user disconnects from the call. CCW is supported on all lines that support the Call Waiting feature, including dual-lines and octo-lines.

This feature is supported in Cisco Unified CME 8.0 and later versions for SCCP IP phones and SCCP analog phones; it is not supported on SIP phones.

For configuration information, see Configure Cancel Call Waiting on SCCP Phone, on page 1288.

Callback Busy Subscriber

This feature allows callers who dial a busy extension number to request a callback from the system when the called number is available. Callers can also request callbacks for extensions that do not answer, and the system will notify them after the called phone is next used.

There can be only one callback request pending against a particular extension number, although a caller can initiate more than one callback to different numbers. If a caller attempts to place a callback request on a number that already has a pending callback request, the caller hears a fast-busy tone. If the called number has call forwarding enabled, the callback request is placed against the final destination number.

No configuration is required for this feature. To display a list of phones that have pending callback requests, use the **show ephone-dn callback** command.

Hunt Groups

Hunt groups allow incoming calls to a specific number (pilot number) to be directed to a defined group of extension numbers.

Incoming calls are redirected from the pilot number to the first extension number as defined by the configuration. If the first number is busy or does not answer, the call is redirected to the next phone in the list. A call continues to be redirected on busy or no answer from number to number in the list until it is answered or until the call reaches the number that is defined as the final number.

The redirect from one directory number to the next in the list is also known as a *hop*. You can set the maximum number of redirects for specific peer or longest-idle hunt groups, and for the maximum number of redirects allowed in a Cisco Unified CME system, both inside and outside hunt groups. If a call makes the maximum number of hops or redirects without being answered, the call is dropped.

In Cisco Unified CME 9.0 and later versions, support for call statistics is added for voice hunt groups. To write all the ephone and voice hunt group statistics to a file, the **ephone-hunt statistics write-all** command is enhanced and renamed to **hunt-group statistics write-all** command. If applicable, the TFTP statistics report consists of both ephone and voice hunt group statistics.

In Cisco Unified CME 9.5 and later versions, the command **hunt-group statistics write-v2** is added to write all ephone hunt group statistics to a file along with total logged in and logged out time for agents. The command was enhanced in Unified CME Release 11.5 to add statistics for total logged in and logged out time for voice hunt group.

The **show telephony-service all** command is also enhanced to display the total number of ephone and voice hunt groups that have statistics collection turned on.

The **statistics collect** command under voice hunt-group configuration mode is introduced to enable the collection of call statistics for a voice hunt group.

The **show voice hunt-group statistics** command is introduced to display call statistics from voice hunt groups.

For Unified CME 11.5 and later versions, the **overwrite-dyn-stats (voice hunt-group)** command is introduced to overwrite statistics of previously joined dynamic agent with stats of newly joined dynamic agents for voice hunt group. The statistics for a dynamic agent are overwritten only when all the 32 available slots are used. For more information, see Cisco Unified Communications Manager Express Command Reference Guide.

For information on displaying statistics for hunt groups, see Cisco Unified CME B-ACD and Tcl Call-Handling Applications.

There are four different types of hunt groups. Each type uses a different strategy to determine the first number that rings for successive calls to the pilot number, as described below.

- Sequential Hunt Groups—Numbers always ring in the left-to-right order in which they are listed when the hunt group is defined. The first number in the list is always the first number to be tried when the pilot number is called. Maximum number of hops is not a configurable parameter for sequential hunt groups. Figure 57: Sequential hunt Group, on page 1250 shows an illustrated example.
- Peer Hunt Groups—The first number to ring is the number to the right of the directory number that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified in the hunt group configuration. Figure 58: Peer hunt Group, on page 1251 shows an illustrated example.
- Longest-Idle Hunt Groups—Calls go first to the number that has been idle the longest for the number of hops specified when the hunt group was defined. The longest-idle time is determined from the last time that a phone registered, reregistered, or went on-hook. Figure 59: Longest-idle hunt Group, on page 1252 shows an illustrated example.
- Parallel Hunt Groups (Call Blast)—Calls ring all numbers in the hunt group simultaneously.

Ephone Hunt-group chains can be configured in any length, but the actual number of hops that can be reached in a chain is determined by the **max-redirect** command configuration. In the following example, a maximum redirect number 15 or greater must be configured for callers to reach the final 5000 number. If a lower number is configured, the call disconnects.

```
ephone-hunt 1 sequential
 pilot 8000
 list 8001, 8002, 8003, 8004
 final 9000

ephone-hunt 2 sequential
 pilot 9000
 list 9001, 9002, 9003, 9004
 final 7000

ephone-hunt 3 sequential
 pilot 7000
 list 7001, 7002, 7003, 7004
 final 5000
```

Cisco Unified CME 4.3 and later versions support the following Voice Hunt-Group features:

- Call Forwarding to a Parallel Voice Hunt-Group (Call Blast)
- Call Transfer to a Voice Hunt-Group
- Member of Voice Hunt-Group can be a SIP phone, SCCP phone, FXS analog phone, DS0-group, PRI-group, or SIP trunk.
- Cisco Unified CME supports chaining (nesting) of a voice hunt group with another voice hunt group. The chaining of voice hunt groups is established by configuring the final number of the first voice hunt group as the pilot number of the second voice hunt group.

Ephone-Hunt Groups and Voice Hunt-Groups Comparison

SIP phones support Voice Hunt-Groups. SCCP phones support Ephone-Hunt Groups, and in Cisco Unified CME 4.3 and later versions, SCCP phones also support Voice Hunt-Groups. Table 104: Feature Comparison of Ephone-Hunt Groups and Voice Hunt-Groups, on page 1250 compares the features of Ephone-Hunt Groups and Voice Hunt-Groups.

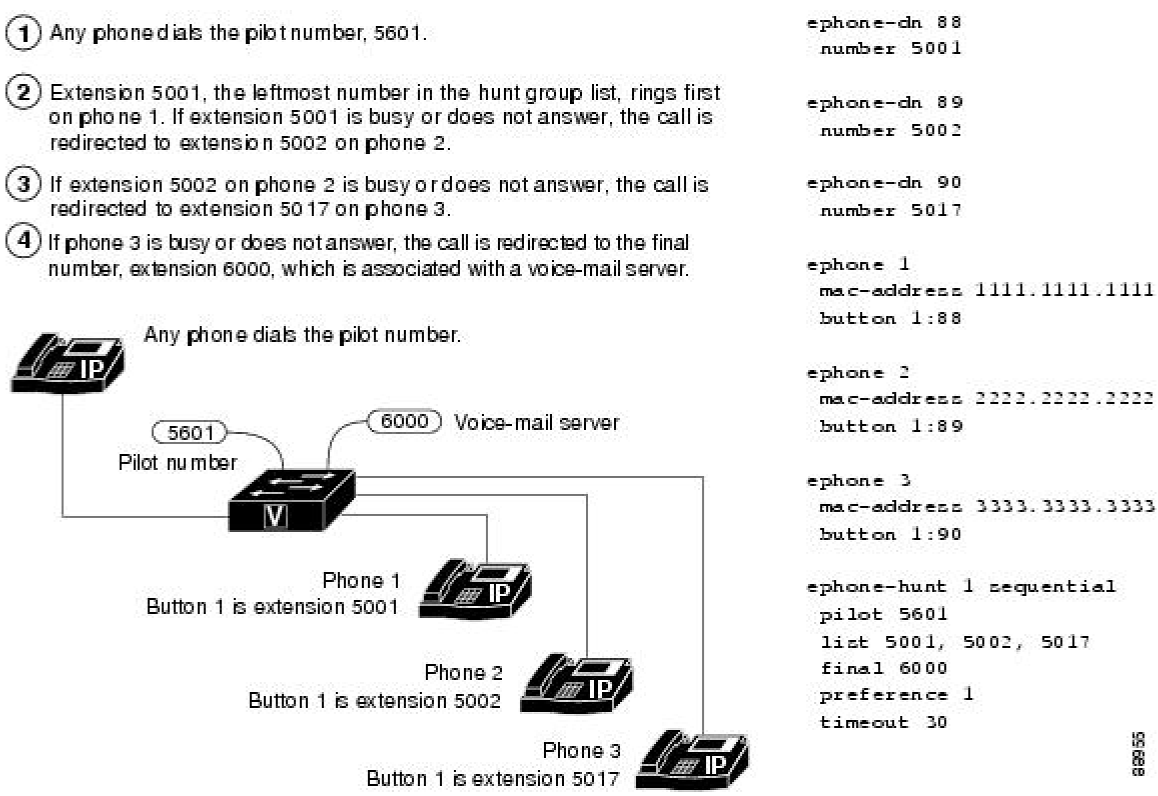
Table 104: Feature Comparison of Ephone-Hunt Groups and Voice Hunt-Groups

Feature	Ephone Hunt	Voice Hunt Group
Endpoints Supported	SCCP only	SIP, SCCP, PSTN, and FXS
Parallel Hunt Groups (Call Blast)	No (for alternative, see Shared-Line Overlays, on page 1275	Yes
Hunt Statistics Support	Yes	Yes
B-ACD Support	Yes	Yes
Features such as present-call and login/logout	Yes	Yes (Only for SIP and SCCP phones)

Sequential Hunt Groups

In a sequential hunt group, extensions always ring in the order in which they are listed, left to right, when the hunt group is defined. The first number in the list is always the first number to be tried when the pilot number is called. Maximum number of hops is not a configurable parameter for sequential hunt groups.

Figure 57: Sequential hunt Group

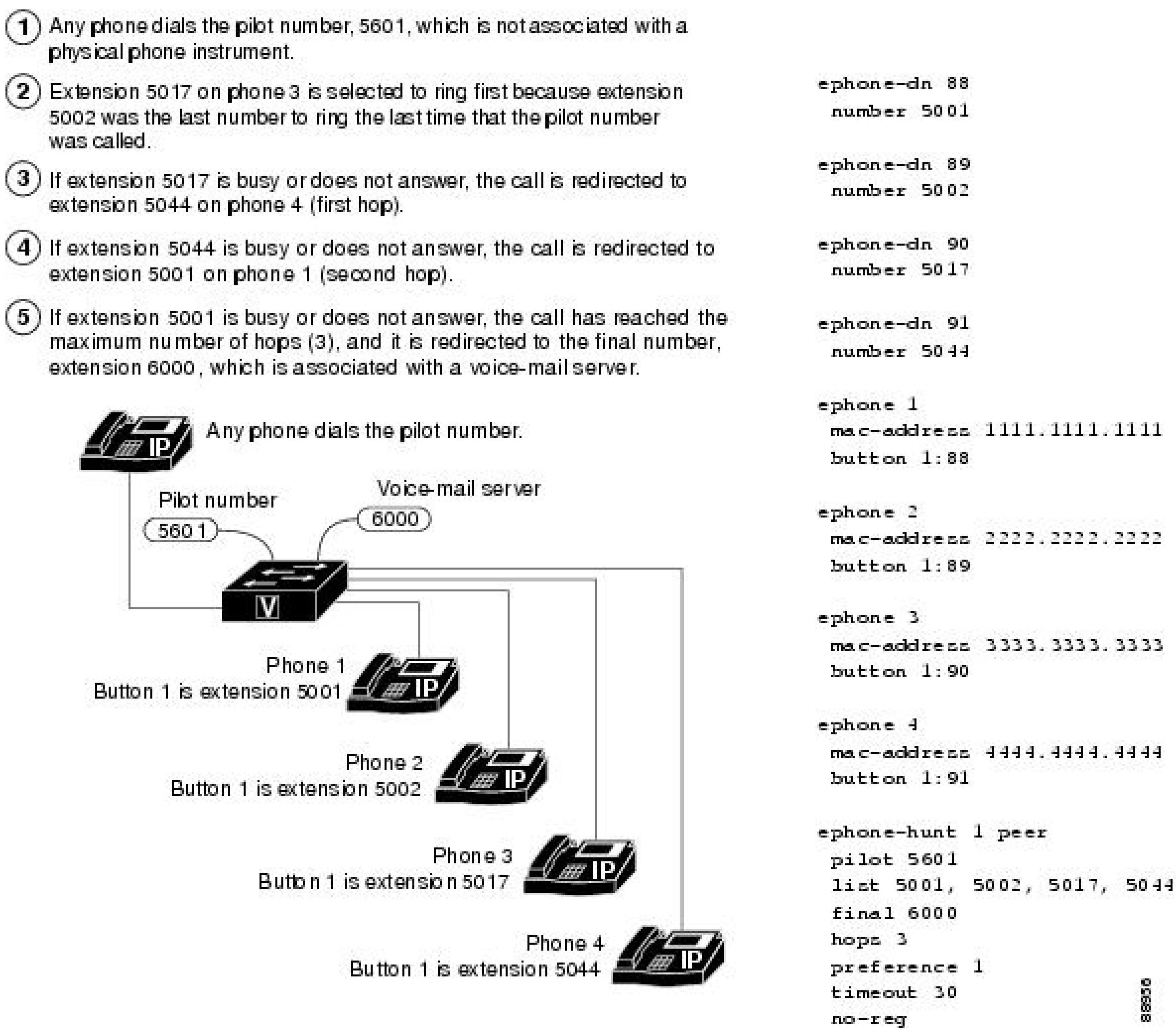


Peer Hunt Groups

In a peer hunt group, extensions ring in a round-robin order. The first extension to ring is the number in the list to the right of the last extension to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified when the hunt group was defined.

Figure 58: Peer hunt Group, on page 1251 illustrates a peer hunt group.

Figure 58: Peer hunt Group



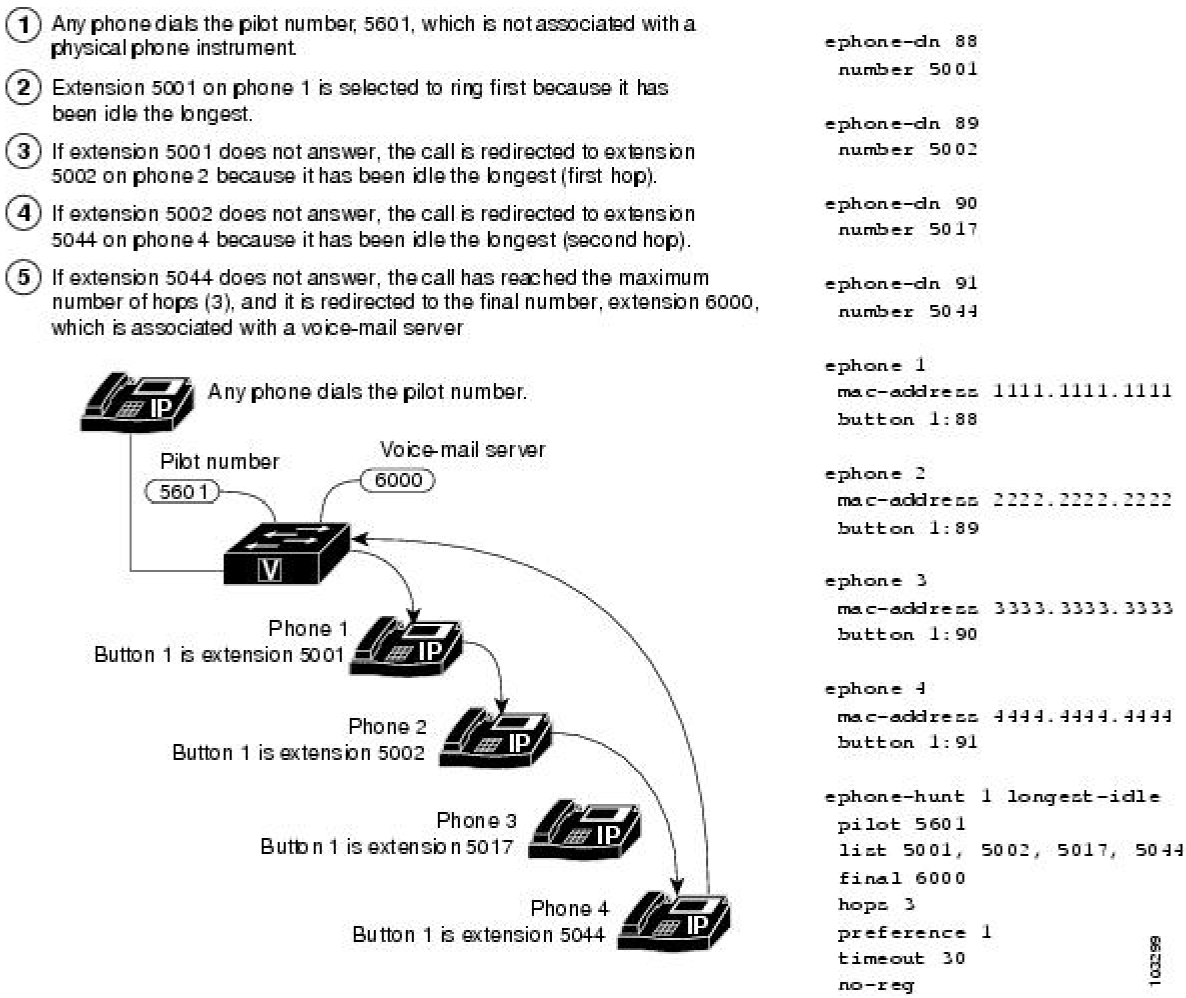
Longest-Idle Hunt Groups

In a longest-idle hunt group, the algorithm for choosing the next extension to receive a call is based on a comparison of on-hook time stamps. The extension with the smallest on-hook time stamp value is chosen when the next call comes to the hunt group.

The default behavior is that an on-hook time stamp value for an extension is updated only when the agent answers a call. In Cisco Unified CME 4.0 and later versions, you can specify that an on-hook time stamp is updated when a call rings an extension and also when a call is answered by an agent.

Figure 59: Longest-idle hunt Group, on page 1252 illustrates a longest-idle hunt group.

Figure 59: Longest-idle hunt Group



Parallel Hunt Groups (Call Blast)

In a parallel hunt group, calls simultaneously ring multiple phones. Using parallel hunt groups is also referred to as application-level forking because it enables the forking of a call to multiple destinations. In versions earlier than Cisco Unified CME 4.3, only SIP phones support parallel hunt groups. In Unified CME 4.3 and later versions, SCCP phones also support voice hunt groups.

You can enable functionality similar to parallel hunt groups on SCCP phones by using the ephone-dn overlay feature for shared lines. See Shared- Line Overlays, on page 1275.

In the following parallel hunt group example, when callers dial extension 1000, extension 1001, 1002, and so on ring simultaneously. The first extension to answer is connected. If none of the extensions answers, the call is forwarded to extension 2000, which is the number for the voice-mail service.

```
voice hunt-group 4 parallel
pilot 1000
list 1001, 1002, 1003, 1004
final 2000
timeout 20
```

The number of ringing calls that a parallel hunt group can support depends on whether call-waiting is enabled on the SIP phones.

If call-waiting is enabled (the default), parallel hunt groups support multiple calls up to the limit of call-waiting calls supported by a particular SIP phone model. You may not want to use unlimited call-waiting, however, with parallel hunt-groups if agents do not want a large number of waiting calls when they are already handling a call.

If call waiting is disabled, parallel hunt groups support only one call at a time in the ringing state. After a call is answered (by one of the phones in the hunt group), a second call is allowed. The second and subsequent calls ring only the idle phones in the hunt group, and bypass the busy phone that answered the first call (because this phone is connected to the first call). After the second call is answered, a third call is allowed, and so on until all the phones in the parallel hunt group are busy. The hunt group does not accept further calls until at least one phone returns to the idle/on-hook state.

When two or more phones within the same parallel hunt group attempt to answer the same call, only one phone can connect to the call. Phones that fail to connect must return to the on-hook state before they can receive subsequent calls. Calls that arrive before a phone is placed on-hook are not presented to the phone. For example, if a second call arrives after Phone 1 has answered the original call, but before Phone 2 goes back on-hook, the second call bypasses Phone 2 (because it is offhook).

When a phone returns to the idle/on-hook state, it does not automatically re-synchronize to the next call waiting to be answered. For example, in the previous scenario, if the second call is still ringing Phone 3 when Phone 2 goes on-hook, Phone 2 does not ring because it was offhook when the second call arrived.

For configuration information, see Configure Voice-Hunt Groups, on page 1301.

View and Join for Voice Hunt Groups

You can view voice hunt group related information on SIP and SCCP phones using the phone menu. The following information related to hunt groups can be viewed on the phone display:

- Name
- Pilot number
- Status

If voice hunt groups have been configured, the user can view the voice hunt group information using the service button on the phone, by navigating to **My Phone Apps** > **Voice Hunt Groups** . On selecting the voice hunt group option, a list of voice hunt groups will be displayed.

A voice hunt group includes the name of the hunt group, the pilot number and also the status of the DN indicating if the DN is a member of the hunt group. This information is displayed in the following method:

- If DN is a static member of the hunt group, then status is displayed with # (hash) symbol.
- If DN is dynamic member, the status is displayed with * (asterisk) symbol.

The following operations can be performed on the phone user interface:

- User can join or unjoin to or from voice hunt groups by selecting the **Join** or **Unjoin** softkey which is displayed on the voice hunt group page. The user can select the required voice hunt group using the up and down buttons.
- User can access the next or previous records of voice hunt groups by selecting the **Next**/**Previous** softkey options.

To display voice hunt-group information on the phone, user needs to configure **phone-display** command under voice hunt-groups.

Restrictions and Limitations

- A DN can join a maximum of six voice hunt groups.
- The displayed hunt group information is applicable only for the primary line of the phone.
- A primary DN can join or unjoin a voice hunt group using the **Service** button on the phone. If a phone is configured with multiple DNs, then DNs other than the primary DN can join the voice hunt groups by dialing the FAC standards.
- The voice hunt group information display feature is applicable only on the phones that support **My Phone Apps** menu. For example, 78xx, 88xx phone families are supported. However, 69xx, 39xx phone families are not supported.

Enable User Interface to View, Join, and Unjoin Voice Hunt Groups on SCCP Phone

This feature enables an SCCP phone user to view information related to the voice hunt groups and join or unjoin voice hunt groups from a menu on their phone. This feature is enabled by default. You must perform this task only if the feature was previously disabled on a phone.

Before You Begin

Cisco Unified CME 10.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **phone-ui voice-hunt-groups**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 4	**phone-ui voice-hunt-groups** **Example:** `Router(config-ephone)# phone-ui voice-hunt-groups`	Enables a SCCP phone user to view information related to voice hunt groups and also join or unjoin from voice hunt groups. • This command is enabled by default.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

The following example shows that the **voice-hunt-groups** command is enabled on an SCCP phone.

```
ephone-dn 10 dual-line
 number 1001
 no huntstop
 huntstop channel
ephone-dn 11 dual-line
```

Note From Cisco Unified CME Release 10.5 onwards, SIP phones will display voice hunt group information, by default.

Configure Service URL Button On SCCP Phone Line Key

To implement service PLK feature line key buttons on Cisco Unified SCCP Phones, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone template** *template-tag*
4. **url-button** *index* **type**| url [name]
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone template** *template-tag* **Example:** `Router(config)# ephone template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.

Step 4	**url-button** *index* **type**| url [name]
	
	Example:
	`Router#(config-ephone-template)#url-button 1 myphoneapp`
	`Router(config-ephone-template)#url-button 2 em`
	`Router(config-ephone-template)#url-button 3 snr`
	`Router(config-ephone-template)#url-button 4 voicehuntgroups`
	`Router(config-ephone-template)#url-button 5 park-list`
	`Router(config-ephone-template)#url-button 6 http://www.cisco.com`
		Configures a service URL feature button on a line key.
		• *Index*—Unique index number. Range: 1 to 8.
		• **type**—Type of service PLK button. The following types of URL service buttons are available:
		◦ myphoneapp: My phone application configured under phone user interface.
		◦ em: Extension Mobility
		◦ snr: Single Number Reach
		◦ voicehuntgroups: Voice Hunt Groups Information
		◦ park-list: Parked calls
		• *url name*—Service URL with maximum length of 31 characters.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)#ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 5`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

The following example shows three URL buttons configured for line keys:

```
!
!
!
ephone-template 5
url-button 1 em
url-button 2 mphoneapp mphoneapp
url-button 3 snr
url-button 4 voicehuntgroups
url-button 5 park-list
!
ephone 36
ephone-template 5
```

What to Do Next

If you are done configuring the url buttons for phones in Cisco Unified CME, restart the phones.

Configure Service URL Button On SIP Phone Line Key

To implement service URL feature line key buttons on Cisco Unified IP Phones, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **url-button** [**index** *number*] [**url** *location*] [*label*]
5. **exit**
6. **voice register pool** *phone-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.

Step 4	**url-button** [**index** *number*] [**url** *location*] [*label*]
	
	Example:
	`Router(config-register-temp)url-button 1 http://x.x.x.x:80/CMEserverForPhone/vhg_root_menu VHG_List`
	`Router(config-register-temp)url-button 2 http://x.x.x.x:80/CMEserverForPhone/park_list Park_List`
		Configures a service url feature button on a line key.
		• x.x.x.x—CME IP address.
		• Index number—Unique index number ranging from 1 to 8.
		• URL *location*—Location of the URL.
		• label—A label name which is displayed on phone.

Step 5	**exit** **Example:** `Router(config-register-temp)# exit`	Exits ephone-template configuration mode.
Step 6	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.

	Command or Action	Purpose
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

The following example shows URL buttons configured in the voice register template 1:

```
Router# show run
!
voice register template  1
url-button 1 http://x.x.x.x:80/CMEserverForPhone/vhg_root_menu VHG_List
url-button 2 http://x.x.x.x:80/CMEserverForPhone/park_list Park_List
url-button 5 http://www.cisco.com Cisco
!
voice register pool 50
!
```

What to Do Next

If you are done configuring the URL buttons for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Display Support for the Name of a Called Voice Hunt-Group

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

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

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

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

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

name SALES

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

name SALES secondary SALES-SECONDARY

Note Use quotes (") when input strings have spaces in between as shown in the next three examples.

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

name "**CUSTOMER SERVICE**" **secondary CS**

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

name FINANCE secondary "**INTERNAL ACCOUNTING**"

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

name "**INTERNAL CALLER**" **secondary** "**EXTERNAL CALLER**"

For configuration information, see Associate a Name with a Called Voice Hunt-Group, on page 1312.

For more configuration examples, see Example for Associating a Name with a Called Voice Hunt-Group, on page 1338.

For configuration information, see Configure Ephone-Hunt Groups on SCCP Phones, on page 1291.

The following **show** commands are modified to reflect the configured primary and secondary pilot names:

- **show ephone-hunt**
- **show voice hunt-group**

The information related to the name of the ephone-hunt group and voice hunt-group are sent to the phone and displayed on the phone's user interface.

Restriction

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

Support for Voice Hunt Group Descriptions

In Cisco Unified CME 9.5, a description can be specified for a voice hunt group using the **description** command in voice hunt-group configuration mode.

For a configuration example, see Example for Specifying a Description for a Voice Hunt-Group, on page 1339.

Prevent Local Call Forwarding to the Final Agent in a Voice Hunt-Groups

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

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

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

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

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

For configuration information, see Prevent Local Call Forwarding to Final Agent in Voice Hunt-Groups, on page 1314.

For a configuration example, see Example for Preventing Local Call Forwarding in Parallel Voice Hunt-Groups, on page 1338.

Enhancement of Support for Voice Hunt Group Agent Statistics

Before Cisco Unified CME Release 11.5, total logged in and total logged out time statistics were supported only for ephone hunt group agents. In Cisco Unified CME 11.5, support for Total logged in and Total logged out time statistics is added for voice hunt group agents also.

- The output of the **show voice-hunt** *tag* **statistics** command is modified to display the additional information in the statistics.

For more configuration examples, see Example for Call Statistics From a Voice Hunt Group, on page 1343.

Enhancement of Support for Ephone-Hunt Group Agent Statistics

Before Cisco Unified CME 9.5, statistics were maintained for each ephone hunt group and each ephone-hunt group agent. Some of the statistics included the number of maximum and minimum agents, average time to answer, average time in a call, and average time on hold.

In Cisco Unified CME 9.5, support for hunt group agent statistics of Cisco Unified SCCP IP phones is enhanced to include the following information:

- Total logged in time—On an hourly basis, displays the duration (in seconds) since a specific agent logged into a hunt group.
- Total logged out time—On an hourly basis, displays the duration (in seconds) since a specific agent logged out of a hunt group.

The output of the **show ephone-hunt** *tag* **statistics** command is modified to display the additional information in the statistics.

For more configuration examples, see Example for Displaying Total Logged-In Time and Total Logged-Out Time for Each Hunt-Group Agent, on page 1339.

Restriction

- Statistics collection for Cisco Unified SCCP and SIP IP phones in Cisco Unified SRST are not supported.

Hunt Group Agent Availability Options

Three options increase the flexibility of hunt group agents by allowing them to dynamically join and leave hunt groups or to temporarily enter a not-ready state in which they do not receive calls.

Table 105: Comparison of Hunt Group Agent Availability Features , on page 1262 compares the following agent availability features:

- Dynamic Ephone Hunt Group Membership, on page 1264
- Dynamically Join or Unjoin Multiple Voice Hunt Groups, on page 1265
- Agent Status Control for Ephone Hunt Group, on page 1266
- Agent Status Control for Voice Hunt Group, on page 1267
- Automatic Agent Status Not-Ready for Ephone Hunt Group, on page 1269

Table 105: Comparison of Hunt Group Agent Availability Features

Comparison Factor	Dynamic Membership	Agent Status Control	Automatic Agent Status Not-Ready
Purpose	Allows an authorized agent to join and leave hunt groups.	Allows an agent to manually activate a toggle to temporarily enter a not-ready state, in which hunt-group calls bypass the agent's phone.	Automatically puts an agent's phone in a not-ready state after a specified number of hunt-group calls are unanswered by the agent's phone.
Example	Agent A joins a hunt group at 8 a.m. and takes calls until 1 p.m., when he leaves the hunt group. While Agent A is a member of the hunt group, he occupies one of the wildcard slots in the list of numbers configured for the hunt group. At 1 p.m., Agent B joins the hunt group using the same wildcard slot that Agent A relinquished when he left.	Agent A takes a coffee break at 10 a.m. and puts his phone into a not-ready status while he is on break. When he returns he puts his phone back into the ready status and immediately starts receiving hunt-group calls again. He retained his wildcard slot while he was in the not-ready status.	Agent B is suddenly called away from her desk before she can manually put her phone into the not-ready status. After a hunt-group call is unanswered at Agent B's phone, the phone is automatically placed in the not-ready status and it is not presented with further hunt-group calls. When Agent B returns, she manually puts her phone back into the ready status.

Comparison Factor	Dynamic Membership	Agent Status Control	Automatic Agent Status Not-Ready
Hunt-group slot availability	An agent joining a hunt group occupies a wildcard slot in the hunt group list. An agent leaving the group relinquishes the slot, which becomes available for another agent.	An agent who enters the not-ready state does not give up a slot in the hunt group. The agent continues to occupy the slot regardless of whether the agent is in the not-ready status.	An agent who enters the not-ready does not give up a slot in the hunt group. The agent continues to occupy the slot regardless of whether the agent is in the not-ready status.
Agent activation method	An authorized agent uses a feature access code (FAC) to join a hunt group and a different FAC to leave the hunt group.	An agent uses the HLog soft key to toggle agent status between ready and not ready. Agents can also use the HLog FAC to toggle between ready and not-ready if FACs are enabled. If the HLog soft key is not enabled, the DND soft key can be used to put an agent in the not-ready status and the agent will not receive any calls.	An agent who is a member of a hunt group configured with the **auto logout** command does not answer the specified number of calls, and the agent's phone is automatically changed to the not-ready status. The agent uses the HLog soft key or a FAC to return to the ready status. If the HLog soft key or FAC has not been enabled in the configuration, the agent uses the DND soft key to return to the ready status.
Configuration	The system administrator uses the **list** command to configure up to 20 wildcard slots in a hunt group and uses the **ephone-hunt login** command to authorize certain directory numbers to use these wildcard slots. See Configure Ephone-Hunt Groups on SCCP Phones, on page 1291.	The system administrator uses the **HLog** keyword with the **hunt-group logout** command to provide an HLog soft key on display phones and uses the **fac** command to enable standard FACs or create a custom FAC. See Configure Ephone-Hunt Groups on SCCP Phones, on page 1291.	The system administrator uses the **auto logout** command to enable automatic agent status not-ready for a hunt group. This functionality is disabled by default. See Configure Ephone-Hunt Groups on SCCP Phones, on page 1291. See Configure Voice-Hunt Groups, on page 1301.

Comparison Factor	Dynamic Membership	Agent Status Control	Automatic Agent Status Not-Ready
Optional customizations	The system administrator can establish custom FACs for agents to use to enter or leave a hunt group.	The system administrator can use the **softkeys** commands to change the position or prevent the display of the HLog soft key on individual phones.	The system administrator can use the **auto logout** command to specify the number of unanswered calls that will trigger an agent status change to not-ready and whether this feature applies to dynamic hunt-group members, static hunt-group members, or both. The system administrator can use the **hunt-group logout** command to specify whether an automatic change to the not-ready status also places a phone in DND mode.

Dynamic Ephone Hunt Group Membership

Hunt groups allow you to set up pools of extension numbers to answer incoming calls. Up to 20 wildcard slots can be entered in the list of hunt group extension numbers to allow dynamic group membership, in which authorized phone users can join a hunt group whenever a vacant wildcard slot is available and they can leave when they like. Each phone user who joins a group occupies one slot. If no slots are available, a user who tries to join a group hears a busy signal.

Allowing dynamic membership in a hunt group is a three-step process:

1. Use the **list** command in ephone-hunt configuration mode to specify up to 20 wildcard slots in the hunt group.
2. Use the **ephone-hunt login** command under each directory number that should be allowed to dynamically join and leave hunt groups. Directory numbers are disallowed from joining ephone hunt groups by default, so you have to explicitly allow this behavior for each directory number that you want to be able to log in to ephone hunt groups.
3. Use the **fac standard** command to enable standard FACs or the **fac custom** command to define custom FACs. FACs must be enabled so that agents can use them to join and leave ephone hunt groups.

To dynamically join an ephone hunt group, a phone user dials a standard or custom FAC for joining an ephone hunt group. The standard FAC to join an ephone hunt group is *3.

If multiple ephone hunt groups have been created that allow dynamic membership, the phone user must also dial the ephone hunt group pilot number. For example, if the following ephone hunt groups are defined, a phone user dials *38000 to join the Sales hunt group:

```
voice hunt-group 24 sequential
pilot 8000
list 8001, 8002, *, *
description Sales Group
final 9000

voice hunt-group 25 sequential
pilot 7000
list 7001, 7002, *, *
description Service Group
final 9000
```

To leave an ephone hunt group, a phone user dials the standard or custom FAC. The standard FAC to leave an ephone hunt group is #3. See Customize Softkeys, on page 925.

Note The Dynamic Membership feature is different from the Agent Status Control feature and the Automatic Agent Status Not-Ready feature. Table 105: Comparison of Hunt Group Agent Availability Features , on page 1262 compares the features.

Dynamically Join or Unjoin Multiple Voice Hunt Groups

In Cisco Unified CME 10.5 and later versions, support for phones to dynamically join the voice hunt groups is added. This feature is supported on both the SIP and SCCP phones. A single DN can dynamically join and unjoin multiple voice hunt groups. You can perform this action on a maximum of six different voice hunt groups.

A single SCCP or SIP DN can join multiple voice hunt groups dynamically by using the existing FAC standards with pilot number of voice hunt groups. A primary DN of a phone can also join and unjoin the voice hunt group using the Join or Unjoin soft key that are available on the Voice Hunt Group information display page in the My Phone App menu by using the service button.

From Cisco Unified CME Release 10.5 onwards, a status message is displayed on the SCCP phone when a dynamic agent joins a hunt group. The support for status message display for a dynamic agent joining a hunt group on the SIP phone is supported from Cisco Unified CME Release 11.6 onwards.

Hunt groups allow you to set up pools of extension numbers to answer incoming calls. You can enter up to 32 wildcard slots in the list of voice hunt group extension numbers to allow dynamic group membership, in which phone users can join or unjoin a voice hunt group whenever a vacant wildcard slot is available. Each phone user who joins a group occupies one slot. If no slots are available, a user who tries to join a group will fail to join.

Allowing dynamic membership in a voice hunt group is a three-step process:

1. Use the **list** command in voice-hunt configuration mode to specify up to 32 wildcard slots in the hunt group.
2. Use the **voice-hunt-groups login** command under each directory number that should be allowed to dynamically join and unjoin hunt groups. Directory numbers are not allowed from joining voice hunt groups by default, so you have to explicitly allow this behavior for each directory number that you want to be able to join or unjoin a voice hunt groups.

3 Use the **fac standard** command to enable standard FACs or the **fac custom** command to define custom FACs. FACs must be enabled so that agents can use them to join and unjoin hunt groups.

To dynamically join a voice hunt group, a phone user dials a standard or custom FAC for joining a voice hunt group. The standard FAC to join a voice hunt group is *3.

If multiple voice hunt groups have been configured with dynamic agents, the phone user must also dial the voice hunt group pilot number. If only one voice hunt group is configured with dynamic agent, on SIP phone only FAC is sufficient. Whereas, on SCCP phone, pilot number is mandatory. For example, if the following voice hunt groups are defined, a phone user dials *38000 to join the Sales hunt group:

```
voice hunt-group 24 sequential
pilot 8000
list 8001, 8002, *, *
description Sales Group
final 9000

voice hunt-group 25 sequential
pilot 7000
list 7001, 7002, *, *
description Service Group
final 9000
```

To unjoin a voice hunt group, a phone user dials the standard or custom FAC. The standard FAC to unjoin from all the hunt groups is #3. See Customize Softkeys, on page 925. If a DN joins multiple voice hunt groups, then to unjoin from a specific voice hunt group the user can dial the standard FAC #4 followed by the pilot number.

Agent Status Control for Ephone Hunt Group

The Agent Status Control feature allows ephone hunt group agents to control whether their phones are in the ready or not-ready status. A phone in the ready status is available to receive calls from the hunt group. A phone in the not-ready status blocks calls from the hunt group. Agents should use the not-ready status for short breaks or other temporary interruptions during which they do not want to receive hunt-group calls.

Agents who put their phones into the not-ready status do not relinquish their slots in the hunt group list.

Agents use the HLog soft key or the DND soft key to put a phone into the not-ready status. When the HLog soft key is used to put a phone in the not-ready status, it does not receive hunt group calls but can receive other calls. If the DND soft key is used, the phone does not receive any calls until it is returned to the ready status. The HLog and DND soft keys toggle the feature: if the phone is in the ready status, pressing the key puts the phone in the not-ready status and vice-versa.

The DND soft key is visible on phones by default, but the HLog soft key must be enabled in the configuration using the **hunt-group logout** command, which has the following options:

- **HLog**—Enables both an HLog soft key and a DND soft key on phones in the idle, seized, and connected call states. When you press the HLog soft key, the phone is changed from the ready to not-ready status or from the not-ready to ready status. When the phone is in the not-ready status, it does not receive calls from the hunt group, but it is still able to receive calls that do not come through the hunt group (calls that directly dial its extension). The DND soft key is also available to block all calls to the phone if that is the preferred behavior.
- **DND**—Enables only a DND soft key on phones. The DND soft key also changes a phone from the ready to not-ready status or from the not-ready to ready status, but the phone does not receive any incoming calls, including those from outside hunt groups.

Phones without soft-key displays can use a FAC to toggle their status from ready to not-ready and back to ready. The **fac** command is configured under telephony-service configuration mode to enable the standard set of FACs or to create custom FACs. The standard FAC to toggle the not-ready status at the directory number (extension) level is *4 and the standard FAC to toggle the not-ready status at the ephone level (all directory numbers on the phone) is *5. See Where to Go Next, on page 1352.

Note The Agent Status Control feature is different from the Dynamic Membership feature and the Automatic Agent Status Not-Ready feature. Table 105: Comparison of Hunt Group Agent Availability Features , on page 1262 compares the features.

Agent Status Control for Voice Hunt Group

The Agent Status Control feature allows voice hunt group agents to control whether their phones are in the ready or not-ready status. A phone in the ready status is available to receive calls from the hunt group. A phone in the not-ready status blocks calls from the hunt group. Agents should use the not-ready status for short breaks or other temporary interruptions during which they do not want to receive hunt-group calls.

Agents who put their phones into the not-ready status do not relinquish their slots in the hunt group list.

Agents use the HLog softkey or the DND softkey to put a phone into the not-ready status. When the HLog softkey is used to put a phone in the not-ready status, it does not receive hunt group calls but can receive other calls. When Agent use DND button, phone will be put into Not-Ready state and Hunt group calls will not be routed. However normal or direct calls are still routed, but without audio notifications.

The DND softkey is visible on phones by default, but the HLog softkey must be enabled in the configuration using the **hunt-group logout** command, which has the following options:

- **HLog—**Enables both an HLog softkey and a DND softkey on phones in the idle, ringing, and connected call states. When you press the HLog softkey, the phone is changed from the ready to not-ready status or from the not-ready to ready status. When the phone is in the not-ready status, it does not receive calls from the hunt group, but it is still able to receive calls that do not come through the hunt group (calls that directly dial its extension). DND softkey suppresses audio notifications for direct calls.
- **DND—**Enables only a DND softkey on phones. The DND softkey also changes a phone from the ready to not-ready status or from the not-ready to ready status for voice hunt group calls. Phones receive those calls that directly dial the extension.

Phones without soft-key displays can use a FAC to toggle their status from ready to not-ready and back to ready. The **fac** command configured under telephony-service configuration mode must be used to enable the standard set of FACs or to create custom FACs. The standard FAC to toggle the not-ready status is *4 and the standard FAC to toggle the not-ready status at the phone level (all directory numbers on the phone) is *5. See Where to Go Next, on page 1352.

From Cisco Unified CME 10.5 onwards, SCCP and SIP phones are supported with Agent Status Control for voice hunt group. SCCP phone can log in or log out to or from voice hunt groups using HLog or DND softkeys, or standard or custom FACs, at line-Level as well as phone level. Whereas, SIP phones can log in or log out to or from voice hunt groups using only standard or custom FACs, only at Line-Level.

From Cisco Unified CME Release 11.6 onwards, SIP phones are also supported with agent status control, for voice hunt groups with HLog softkeys or FAC. Hence, SIP phones can logout or login to voice hunt group using HLog softkey, feature button, or FAC at phone level. If the phone is configured with a single line or multiple lines, and if these lines are members of a voice hunt group, then phone level logout or login results in logout or login of all lines on the phone.

To make HLog functionality work with the SIP or SCCP phones, you need to configure the command **hunt-group logout HLog** under telephony-service. Once user is logged out from the hunt group, phone displays a message stating that the user is logged out of hunt group. When the user is logged in to hunt group, the agent phone displays a message stating that the user is logged in to hunt group. For Unified CME 12.1 and earlier releases, if any directory number that is part of voice hunt group is shared across phones, then logout is not allowed at the phone level.

To enable FAC, you need to configure standard or custom FAC under telephony service configuration mode using the command **fac standard** or **fac custom**.

SIP and SCCP phone behavior is different for the following scenarios:

- If phone dn's are not members of a hunt group and phone is configured with an HLog feature button, then phone LED is off for SIP phones and on for SCCP phones.
- If a SIP phone is already in logged in state, any newly joining dn of that phone (in any voice hunt group) is automatically in logged in state.
- If a SIP phone is already in logged out state, any newly joining dn of that phone (in any voice hunt group) is automatically in logged out state.
- Irrespective of whether the SCCP phone is in logged out or logged in state, any dn of that phone joining any voice hunt group retains its previous state (logged out or logged in). For example, if dn 8002 is member of voice hunt group 1 in logged out state, then 8002 remains in logged out state on joining voice hunt group 2. If dn 8001 on the same phone (which was not part of any hunt group) joins any voice hunt group, it is in logged in state.

Note From Cisco Unified CME Release 11.6 onwards, line level logout or login using FAC *4 is not supported for SIP phones (only supported on SCCP phones). SIP phones only support phone level logout or login using FAC *5.

Use **hlog-block** command under **voice hunt-group** for Agent Status Control. If you enable this command under **voice hunt-group**, the logout or login functionality for voice hunt-group is disabled. For example, you can use **hlog-block** command in voice hunt-groups where logout or login functionality using HLog softkey (or by using FAC) needs to be restricted. By default, **hlog-block** command is disabled.

Note The Agent Status Control feature is different from the Dynamic Membership feature and the Automatic Agent Status Not-Ready feature. Table 105: Comparison of Hunt Group Agent Availability Features , on page 1262 compares the features.

Members Logout for Ephone Hunt Group

All members configured under an ephone-hunt are initialized with HLogin by default. The non-shared static members or agents in an ephone hunt group can be configured with the Hlogout initial state using the Members Logout feature. You can use the CLI command **members logout** configured under ephone-hunt configuration mode to enable the feature. From Cisco Unified CME Release 9.1, members logout is supported for ephone hunt groups.

Members logout cannot be used for shared DNs. Also, this feature is not supported if the CLI commands **list** and **hunt-group logout DND** are configured.

Members Logout for Voice Hunt Group

All members configured in a voice hunt group are initialized with HLogin by default. The non-shared static members or agents in a voice hunt group can be configured with the Hlogout initial state using members logout functionality. You can use the CLI command **members logout** configured under voice hunt group configuration mode to enable the feature. From Cisco Unified CME Release 11.6, members logout is supported in voice hunt groups.

If any member of a hunt group in a SIP phone logs out using the CLI command **members logout**, all other DN's of that phone in any hunt group are also logged out. This is because SIP phones only support phone level logout. For SCCP phones, only the DN that is configured with the CLI command **members logout** is logged out from the hunt group. Other member DN's do not logout as SCCP phones support line level logout.

Members logout cannot be used for shared DNs. The feature is not supported if the CLI command **hunt-group logout DND** is configured. Also, you cannot configure the CLI command **members logout** if the command **list** is configured.

Automatic Agent Status Not-Ready for Ephone Hunt Group

Before Cisco Unified CME 4.0, this feature was known as Automatic Hunt Group Logout. If the **auto logout** command was enabled for a hunt group, a phone was placed in DND mode when a line on the phone did not answer a call for that hunt group within the time limit specified in the **timeout** command.

In Cisco Unified CME 4.0 and later versions, the name and behavior of this feature has changed, although the Cisco IOS command remains the same. The **auto logout** command now specifies the number of unanswered hunt group calls after which the agent status of an directory number is automatically changed to not-ready. You can limit Automatic Agent Status Not-Ready to dynamic hunt group members (those who log in using a wildcard slot in the **list** command) or to static hunt group members (those who are explicitly named in the **list** command), or you can apply this behavior to all hunt group members.

A related command, **hunt-group logout**, specifies whether the phones that are automatically changed to the not-ready status should also be placed into DND mode. Phones in the not-ready status do not accept calls from hunt groups, but they do accept calls that directly dial their extensions. Phones in DND mode do not accept any calls. The default if the **hunt-group logout** command is not used is that the phones that are automatically placed in the not-ready status are also placed in DND mode.

Agents whose phones are automatically placed into the not-ready status do not relinquish their slots in the hunt group list.

Note The Automatic Agent Status Not-Ready feature is different from the Dynamic Membership feature and the Agent Status Control feature. Table 105: Comparison of Hunt Group Agent Availability Features , on page 1262 compares the features.

Automatic Agent Status Not-Ready for Voice Hunt Group

From Cisco Unified CME Release 11.6, Automatic Hunt Group Logout is supported on voice hunt groups. If the **auto logout** CLI command is enabled for a hunt group, it specifies the number of successive unanswered hunt group calls after which the agent status of an directory number is automatically changed to not-ready. The range for the number of unanswered rings configured under **auto logout** command is 1 to 20. If auto logout is not configured with any value, the default value of 1 is applied.

When the **auto logout** command is enabled under voice hunt group, the auto logout behavior applies to all hunt group members (including static and dynamic members).

A related command, **hunt-group logout**, specifies whether the phones are automatically changed to the not-ready status. Phones in the not-ready state do not accept calls from hunt groups, but they do accept calls that directly dial their extensions.

If **hunt group logout HLog** is configured, then the DNs of that hunt group will go to logout state when the number of unanswered rings specified under **auto logout** command is exceeded. If **hunt group logout DND** is configured, then phone goes to DND mode and logs out the DND member when the number of unanswered rings specified under **auto logout** command is exceeded. If any hunt group members are logged out, they can use HLog Softkey, FAC, Feature Button, or DND softkey to login again.

Agents whose phones are automatically placed into the not-ready status do not relinquish their slots in the hunt group list. When an agent returns to ready status, the voice hunt group resumes sending calls to the agent's DN.

Consider a voice hunt group in sequential, peer, or longest idle configuration mode with call hunt in progress. Then, auto logout count is incremented for agents who do not answer the call. The auto logout count is not incremented for agents who answer the call. In this scenario, the agent can be either an SCCP DN or a SIP DN.

Consider a voice hunt group in parallel configuration mode with call blast in progress to all logged in DN's in the hunt group. If call is answered by any of the agents, then the remaining agents in that hunt group will not have auto logout count incremented. However, if call is not answered by any of the agents, then the auto logout count will be incremented for all the logged in agents. Here, agent can be either a SCCP DN or SIP DN.

Note The Automatic Agent Status Not-Ready feature is different from the Dynamic Membership feature and the Agent Status Control feature. Table 105: Comparison of Hunt Group Agent Availability Features , on page 1262 compares the features.

Presentation of Calls for Ephone Hunt Group

For phones configured under ephone hunt group configuration mode, presentation of calls is supported using the CLI command, **present-call** . When the CLI command is configured, calls from the ephone hunt group are presented only if all lines are on hook or in idle state.

If you configure **idle-phone** as the sub-mode option of the CLI command **present-call** , calls from the ephone-hunt group are presented only if all lines are idle on the phone on which the hunt-group line appears. This option does not consider monitored lines that have been configured on the phone using the **button m** command.

If you configure **onhook-phone** as the sub-mode option of the CLI command **present-call** , calls from the ephone-hunt group are presented only if the phone on which the number appears is in onhook state. When this keyword is configured, calls in the ringing or hold state that are unrelated to the hunt group do not prevent the presentation of calls from the ephone-hunt group.

Presentation of Calls for Voice Hunt Group

For phones configured under voice hunt group configuration mode, presentation of calls is supported using the CLI command **present-call** . The feature is supported from Cisco Unified CME Release 11.6 onwards.

When the **present-call** CLI command is configured, calls from the voice hunt group are presented only if all lines are idle on the phone on which the hunt group line appears.

If the **present-call** CLI command is not configured, voice hunt group calls are presented without considering the status of other phone lines on the phone. Hence, voice hunt group presents calls to an ephone or voice register pool whenever the phone line (ephone-dn or voice register dn) that corresponds to a number in a voice hunt group list is available. Hence, when you configure the **present-call** CLI command, you get the additional control to ensure that hunt group calls do not possibly go unanswered.

Night Service

The night-service feature allows you to provide coverage for unstaffed extensions during hours that you designate as "night-service" hours. During the night-service hours, calls to the designated extensions, known as night-service directory numbers or night-service lines, send a special "burst" ring (for SCCP phones and SIP phones) to night-service phones that have been specified to receive this special ring. Phone users at the night-service phones can then use the call-pickup feature to answer the incoming calls from the night-service directory numbers.

For example, the night-service feature can allow an employee working after hours to intercept and answer calls that are presented to an unattended receptionist's phone. This feature is useful for sites at which all incoming public switched telephone network (PSTN) calls have to be transferred by a receptionist. This is because all the Direct Inward Dialing (DID) calls are not published to PSTN for Cisco Unified CME system. When a call arrives at the unattended receptionist's phone during hours that are specified as night service, a ring burst notifies a specified set of phones of the incoming call. A phone user at any of the night-service phones can intercept the call using the call-pickup feature. Night-service call notification is sent every 12 seconds until the call is either answered or aborted.

A user can enter a night-service code to manually toggle night-service treatment off and on from any phone that has a line assigned to night service. Before Cisco CME 3.3, using the night-service code turns night service on or off only for directory numbers on the phone at which the code is entered. In Cisco CME 3.3 and later versions, using the night-service code at any phone with a night-service directory number turns night service on or off for all phones with night-service directory numbers. From Unified CME 11.5 onwards, night service feature is supported on SIP phones along with SCCP phones.

Mixed deployment of SIP and SCCP phones is supported from Cisco Unified CME Release 11.6. Any combination of SIP and SCCP phones are supported across incoming call, unstaffed DNs, and agent phones. For DNs in which night service is enabled, notifications are sent to both SIP and SCCP phones that are designated as night service agents in a mixed deployment.

[Figure 60: Night Service for SCCP Phones, on page 1272](#) illustrates night service for SCCP phones.

Figure 60: Night Service for SCCP Phones

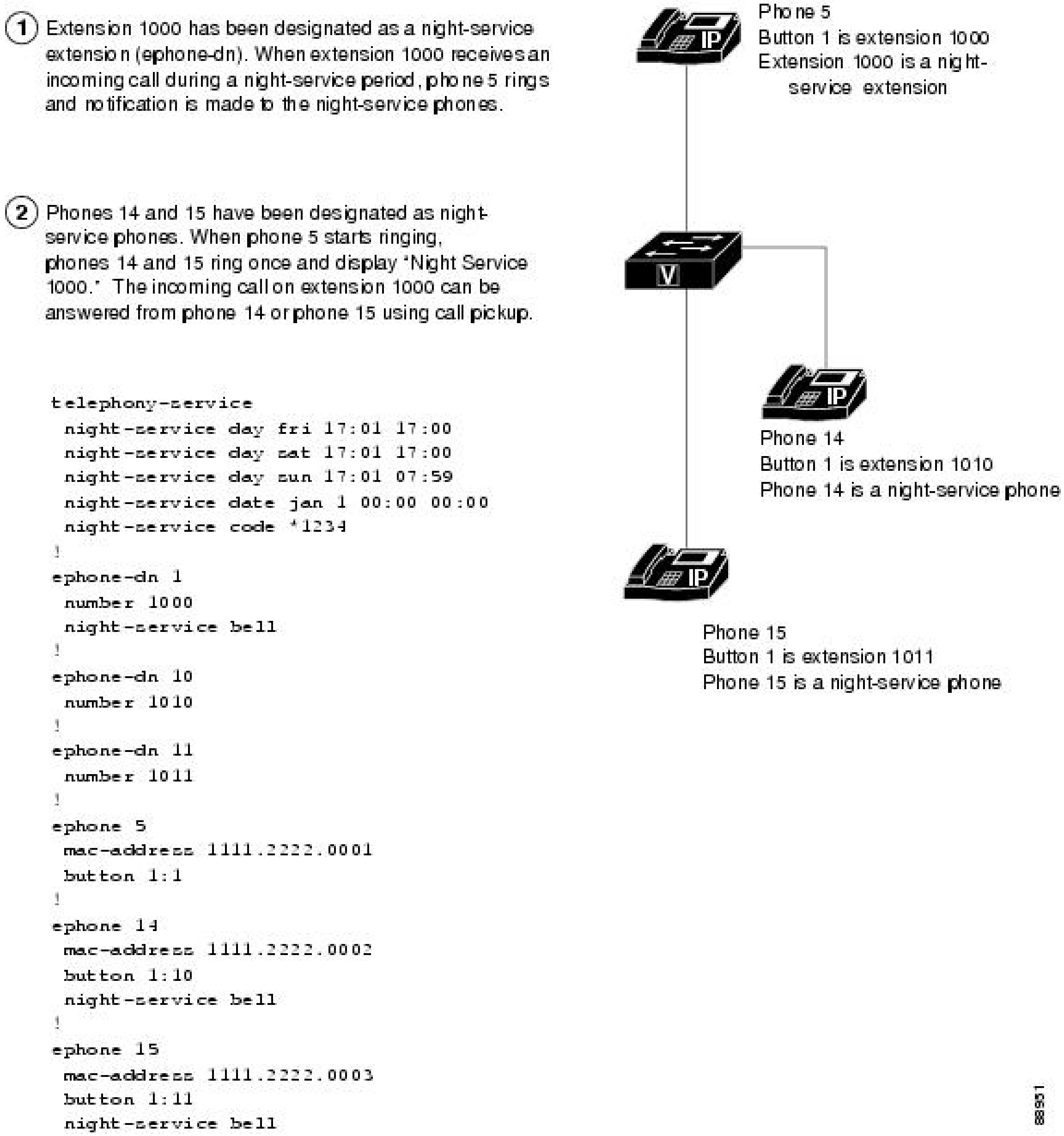
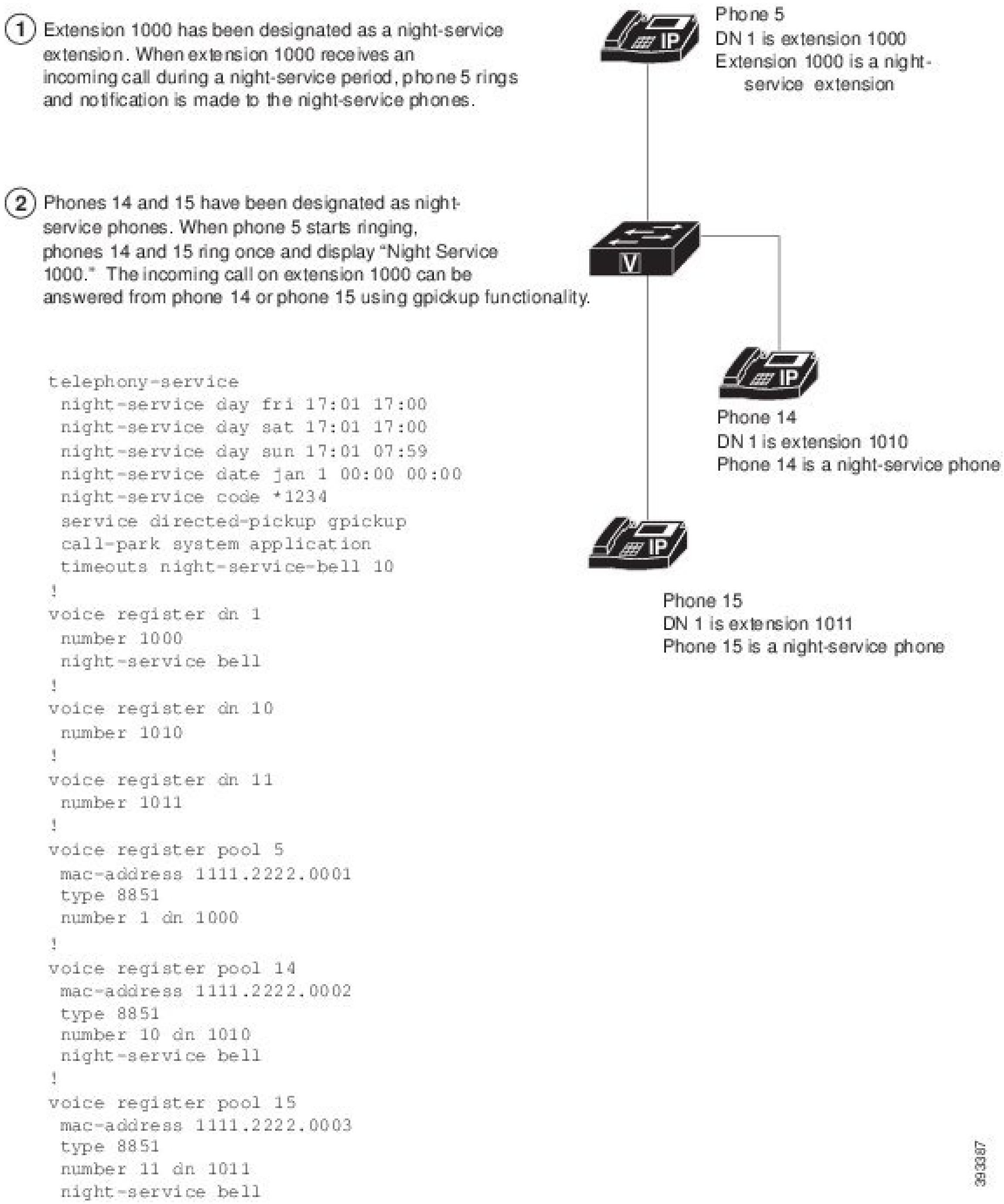


Figure 61: Night Service for SIP Phones, on page 1273 illustrates night service for SIP phones.

Figure 61: Night Service for SIP Phones



Overlaid Ephone-dns

Overlaid ephone-dns are directory numbers that share the same button on a phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls. Up to 25 ephone-dns can be assigned to a single phone button. They can have the same extension number or different numbers. The same ephone-dns can appear on more than one phone and more than one phone can have the same set of overlaid ephone-dns.

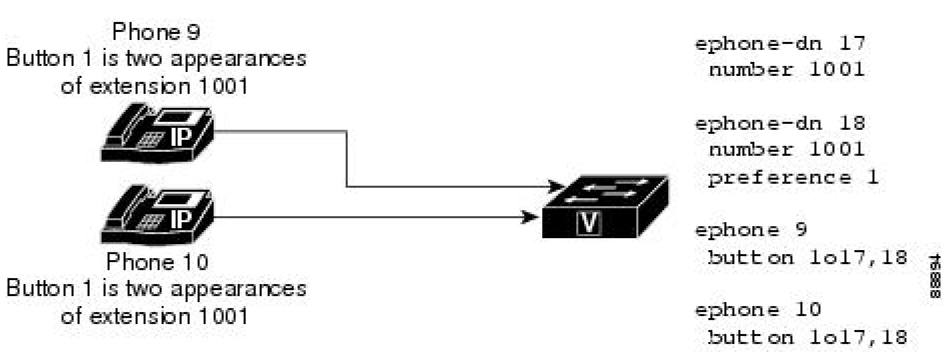
The order in which overlaid ephone-dns are used by incoming calls can be determined by the call hunt commands, **preference** and **huntstop**. For example, ephone-dn 1 to ephone-dn 4 have the same extension number, 1001. Three phones are configured with the **button 1o1,2,3,4** command. A call to 1001 will ring on the ephone-dn with the highest preference and display the caller ID on all phones that are on hook. If another incoming call to 1001 is placed while the first call is active (and the first ephone-dn with the highest preference is configured with the **no huntstop** command), the second call will roll over to the ephone-dn with the next-highest preference, and so forth. For more information, see Call Hunt, on page 1243.

If the ephone-dns in an ephone-dn overlay use different numbers, incoming calls go to the ephone-dn with the highest preference. If no preferences are configured, the **dial-peer hunt** command setting is used to determine which ephone-dns are used for incoming calls. The default setting for the **dial-peer hunt** command is to randomly select an ephone-dn that matches the called number.

Note To continue or to stop the search for ephone-dns, you must use, respectively, the **no huntstop** and **huntstop** commands under the individual ephone-dns. The huntstop setting is applied only to the dial peers affected by the **ephone-dn** command in telephony-service mode. Dial peers configured in global configuration mode comply with the global configuration huntstop setting.

Figure 62: Overlaid Ephone-dn (Simple Case), on page 1274 shows an overlay set with two directory numbers and one number that is shared on two phones. Ephone-dn 17 has a default preference value of 0, so it will receive the first call to extension 1001. The phone user at phone 9 answers the call, and a second incoming call to extension 1001 can be answered on phone 10 using directory number 18.

Figure 62: Overlaid Ephone-dn (Simple Case)



When a call is answered on an ephone-dn, that ephone-dn is no longer available to other phones that share the ephone-dn in overlay mode. For example, if extension 1001 is answered by phone 1, caller ID for extension 1001 displays on phone 1 and is removed from the screens of phone 2 and phone 3. All actions pertaining to the call to extension 1001 (ephone-dn 17) are displayed on phone 1 only. If phone 1 puts extension 1001 on hold, the other phones will not be able to pick up the on-hold call using a simple shared-line pickup. In addition, none of the other four phones will be able to make outgoing calls from the ephone-dn while it is in use. When phone users press button 1, they will be connected to the next available ephone-dn listed in the **button** command. For example, if phone 1 and phone 2 are using ephone-dn 1 and ephone-dn 2, respectively, phone 3 must pick up ephone-dn 3 for an outgoing call.

If there are more phones than ephone-dns associated with an ephone-dn overlay set, it is possible for some phones to find that all the ephone-dns within their overlay set are in use by other phones. For example, if five phones have a line button configured with the **button 1o1, 2, 3** command, there may be times when all three of the ephone-dns in the overlay set are in use. When that occurs, the other two phones will not be able to use an ephone-dn in the overlay set. When all ephone-dns in an overlay set are in use, phones with this overlay set will display the remote-line-in-use icon (a picture of a phone with a flashing X through it) for the corresponding line button. When at least one ephone-dn becomes available within the overlay set (that is, an ephone-dn is either idle or ringing), the phone display reverts to showing the status of the available ephone-dn (idle or ringing).

Shared- Line Overlays

Dual-line ephone-dns can also use overlays. The configuration parameters are the same as for single-line ephone-dns, except that the **huntstop channel** command must be used to keep calls from hunting to the ephone-dn's second channel.

The primary ephone-dn in a shared-line overlay set should be unique to the phone to guarantee that the phone has a line available for outgoing calls, and to ensure that the phone user can obtain dial-tone even when there are no idle lines available in the rest of the shared-line overlay set. Use a unique ephone-dn to provide for a unique calling party identity on outbound calls made by the phone so that the called user can see which specific phone is calling.

The following example shows the configuration for a simple shared-line overlay set. The primary ephone-dn that is configured for each phone is unique while the remaining ephone-dns 10, 11, and 12 are shared in the overlay set on both phones.

```
ephone 1
 mac-address 1111.1111.1111
 button 1o1,10,11,12
!
ephone 2
 mac-address 2222.2222.2222
 button 1o2,10,11,12
```

A more complex directory number configuration mixes overlaid directory numbers with shared directory numbers and plain dual-line directory numbers on the same phones. Figure 63: Overlaid Ephone-dn (Complex Case), on page 1276 illustrates the following example of a manager with two assistants. On the manager's phone the same number, 2001, appears on button 1 and button 2. The two line appearances of extension 2001 use two single-line directory numbers, so the manager can have two active calls on this number simultaneously, one on each button. The directory numbers are set up so that button 1 will ring first, and if a second call comes in, button 2 will ring. Each assistant has a personal directory number and also shares the manager's directory numbers. Assistant 1 has all three directory numbers in an overlay set on one button, whereas assistant 2 has one button for the private line and a second button with both of the manager's lines in an overlay set. A sequence of calls might be as follows.

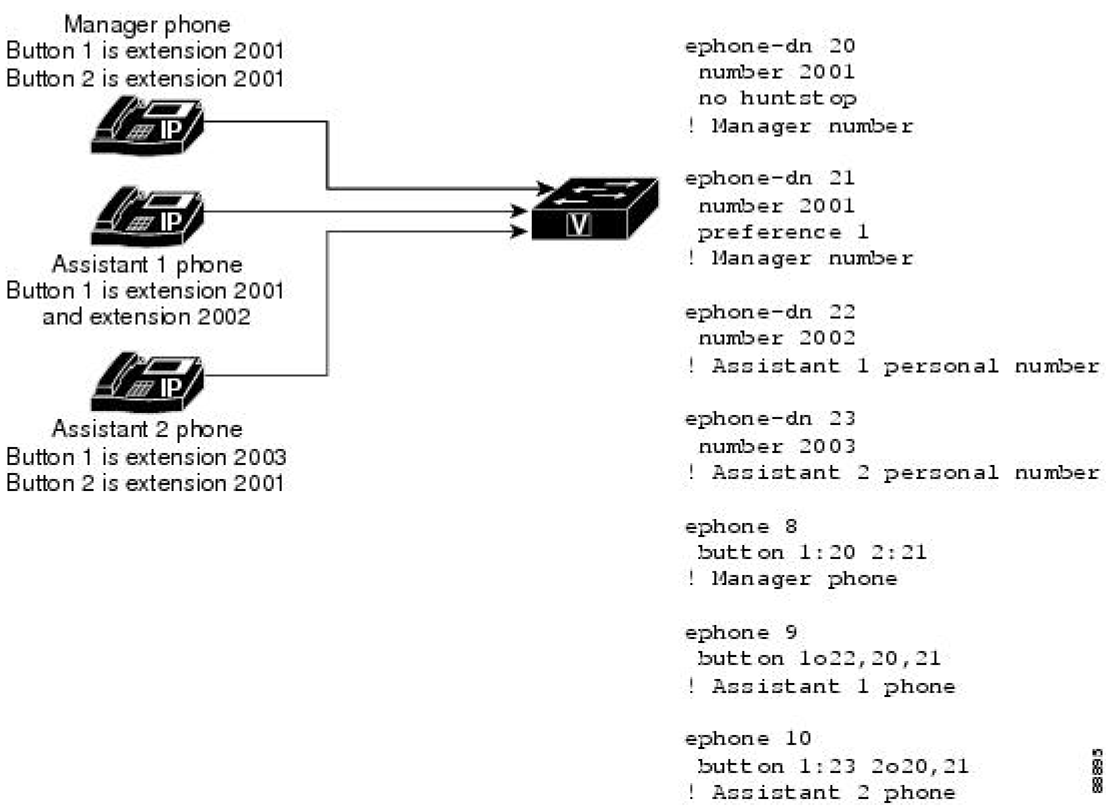
1. An incoming call is answered by the manager on extension 2001 on button 1 (directory number 20).
2. A second call rings on 2001 and rolls over to the second button on the manager's phone (directory number 21). It also rings on both assistants' phones, where it is also directory number 21, a shared directory number.

3 Assistant 2 answers the call. This is a shared overlay line (one directory number, 21, is shared among three phones, and on two of them this directory number is part of an overlay set). Because it is shared with button 2 on the manager's phone, the manager can see when assistant 2 answers the call.

4 Assistant 1 makes an outgoing call on directory number 22. The button is available because of the additional directory numbers in the overlay set on the assistant 1 phone.

At this point, the manager is in conversation on directory number 20, assistant 1 is in conversation on directory number 22, and assistant 2 is in conversation on directory number 21.

Figure 63: Overlaid Ephone-dn (Complex Case)



For configuration information, see Configure Overlaid Ephone-dns on SCCP Phones, on page 1326.

Call Waiting for Overlaid Ephone-dns

Call waiting allows phone users to know that another person is calling them while they are talking on the phone. Phone users hear a call-waiting tone indicating that another party is trying to reach them. Calls to IP phones with soft keys can be answered with the Answer soft key. Calls to analog phones are answered using hookflash. When phone users answer a call-waiting call, their original call is automatically put on hold. If phone users ignore a call-waiting call, the caller is forwarded if call-forward no-answer has been configured.

In Cisco CME 3.2.1 and later versions, call waiting is available for overlaid ephone-dns. The difference in configuration between overlaid ephone-dns with call waiting and overlaid ephone-dns without call waiting is that overlaid ephone-dns with call waiting use the c keyword in the button command and overlaid ephone-dns without call waiting use the o keyword. For configuration information, see Configure Overlaid Ephone-dns on SCCP Phones, on page 1326.

The behavior of overlaid ephone-dns with call waiting and overlaid ephone-dns without call waiting is the same, except for the following:

- Calls to numbers included in overlaid ephone-dns with call waiting will cause inactive phones to ring and active phones connected to other parties to generate auditory call-waiting notification. The default sound is beeping, but you can configure an ephone-dn to use a ringing sound. (See Configure Call-Waiting Indicator Tone on SCCP Phone, on page 1285.) Visual call-waiting notification includes the blinking of handset indicator lights and the display of caller IDs.

  For example, if three of four phones are engaged in calls to numbers from the same overlaid ephone-dn with call-waiting and another call comes in, the one inactive phone will ring, and the three active phones will issue auditory and visual call-waiting notification.

- In Cisco Unified CME 4.0 and later versions, up to six waiting calls can be displayed on Cisco Unified IP Phone 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G, and 7971G-GE. For all other phones and earlier Cisco Unified CME versions, two calls to numbers in an overlaid ephone-dn set can be announced. Subsequent calls must wait in line until one of the two original calls has ended. The callers who are waiting in the line will hear a ringback tone.

For example, a Cisco Unified IP Phone 7910 (maximum two call-waiting calls) has a button configured with a set of overlaid ephone-dns with call waiting (**button 1c1,2,3,4**). A call to ephone-dn 1 is answered. A call to ephone-dn 2 generates call-waiting notification. Calls to ephone-dn 3 and ephone-dn 4 will wait in line and remain invisible to the phone user until one of the two original calls ends. When the call to ephone-dn 1 ends, the phone user can then talk to the person who called ephone-dn 2. The call to ephone-dn 3 issues call-waiting notification while the call to ephone-dn 4 waits in line. (The Cisco Unified IP Phone 7960 supports six calls waiting.) Phones configured for call waiting do not generate call-waiting notification when they are transferring calls or hosting conference calls.

Note that if an overlaid ephone-dn has call-forward-no-answer configured, calls to the ephone-dn that are unanswered before the no-answer timeout expires are forwarded to the configured destination. If call-forward-no-answer is not configured, incoming calls receive ringback tones until the calls are answered.

More than one phone can use the same set of overlaid ephone-dns. In this case, the call-waiting behavior is slightly different. The following example demonstrates call waiting for overlaid ephone-dns that are shared on two phones:

```
ephone 1
button 1c1,2,3,4
!
ephone 2
button 1c1,2,3,4
```

1. A call to ephone-dn 1 rings on ephone 1 and on ephone 2. Ephone 1 answers, and the call is no longer visible to ephone 2.
2. A call to ephone-dn 2 issues a call-waiting notification to ephone 1 and rings on ephone 2, which answers. The second call is no longer visible to ephone 1.
3. A call to ephone-dn 3 issues a call-waiting notification to ephone 1 and ephone 2. Ephone 1 puts the call to ephone-dn 1 on hold and answers the call to ephone-dn 3. The call to ephone-dn 3 is no longer visible to ephone 2.
4. A call to ephone-dn 4 is issues a call-waiting notification on ephone 2. The call is not visible on ephone 1 because it has met the two-call maximum by handling the calls to ephone-dn 1 and ephone-dn 3. (Note

that the call maximum is six for those phones that are able to handle six call-waiting calls, as previously described.)

Note Ephone-dns accept call interruptions, such as call waiting, by default. For call waiting to work, the default must be active. For more information, see Configure Call-Waiting Indicator Tone on SCCP Phone, on page 1285.

Extend Calls for Overlaid Ephone-dns to Other Buttons on the Same Phone

Phones with overlaid ephone-dns can use the **button** command with the **x** keyword to dedicate one or more additional buttons to receive overflow calls. If an overlay button is busy, an incoming call to any of the other ephone-dns in the overlay set rings on the first available overflow button on each phone that is configured to receive the overflow. This feature works only for overlaid ephone-dns that are configured with the **button** command and the **o** keyword; it is not supported with overlaid ephone-dns that are configured using the **button** command and the **c** keyword or other types of ephone-dns that are not overlaid.

Using the **button** command with the **c** keyword results in multiple calls on one button (the button is overlaid with multiple ephone-dns that have call waiting), whereas using the **button** command with the **o** keyword and the **x** keyword results in one call per button and calls on multiple buttons.

For example, an ephone has an overlay button with ten numbers assigned to it using the **button** command and the **o** keyword. The next two buttons on the phone are configured using the **button** command and the **x** keyword. These buttons are reserved to receive additional calls to the overlaid extensions on the first button when the first button is in use.

```
ephone 276
 button 1o24,25,26,27,28,29,30,31,32,33 2x1 3x1
```

For configuration information, see Configure Overlaid Ephone-dns on SCCP Phones, on page 1326.

Configure Call Coverage Features

Configure Call Hunt on SCCP Phones

To configure a group of directory numbers to provide call coverage for a single called number, perform the following steps for each directory number in the group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **preference** *preference-order* [**secondary** *secondary-order*]
6. **no huntstop** or **huntstop**
7. **huntstop channel**
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	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 20 dual-line`	Enters ephone-dn configuration mode for the purpose of configuring a directory number.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 101`	Associates a telephone or extension number with the directory number. • Assign the same number to several primary or secondary ephone-dns to create a group of virtual dial peers through which the incoming called number must search.
Step 5	**preference** *preference-order* [**secondary** *secondary-order*] **Example:** `Router(config-ephone-dn)# preference 2`	Sets the preference value for the ephone-dn. • Default: 0. • Increment the preference order for subsequent ephone-dns with the same number. That is, the first directory number is preference **0** by default and you must specify **1** for the second ephone-dn with the same number, **2** for the next, and so on. • **secondary** *secondary-order*—(Optional) Preference value for the secondary number of an ephone-dn. Default is 9.

Step 6	**no huntstop** or **huntstop**
	
	Example:
	`Router(config-ephone-dn)# no huntstop`
	or
	`Router(config-ephone-dn)# huntstop`
		Explicitly enables call hunting behavior for a directory number.
		• Configure **no huntstop** for all ephone-dns, *except* the final ephone-dn, within a set of ephone-dns with the same number.
		• Configure the **huntstop** command for the final ephone-dn within a set of ephone-dns with the same number.

Step 7	**huntstop channel** **Example:** `Router(config-ephone-dn)# huntstop channel`	(Optional) Enables channel huntstop, which keeps a call from hunting to the next channel of a directory number if the first channel is busy or does not answer. • Required for dual-line ephone-dns that are used for call hunting.
Step 8	**end**	

	Command or Action	Purpose
	Example: `Router(config-ephone-dn)# end`	

What to Do Next

If you want to collect statistics for hunt groups, see Cisco Unified CME B-ACD and Tcl Call-Handling Applications.

Verify Call Hunt Configuration on SCCP Phones

To verify the configuration for call hunt, perform the following steps.

SUMMARY STEPS

1. **show running-config**
2. **show telephony-service ephone-dn**
3. **show telephony-service all** or **show telephony-service dial-peer**

DETAILED STEPS

Step 1 **show running-config**

This command displays your configuration. Preference and huntstop information is listed in the ephone-dn portion of the output.

`Router#` **show running-config**

```
ephone-dn  2  dual-line
number 126
description FrontDesk
name Receptionist
preference 1
call-forward busy 500
huntstop channel
no huntstop
```

Step 2 **show telephony-service ephone-dn**

This command displays ephone-dn preference and huntstop configuration information.

Step 3 **show telephony-service all** or **show telephony-service dial-peer**

These commands display preference and huntstop configurations for ephone-dn dial peers.

```
Router# show telephony-service dial-peer

!
dial-peer voice 20026 pots
destination-pattern 5002
huntstop
call-forward noan 5001 timeout 45
port 50/0/2
```

Configure Call Hunt on SIP Phones

To configure the call hunting feature and prevent hunt-on-busy from redirecting a call from a busy phone into a dial peer that has been setup with a catch-all default destination, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **preference** *preference-order*
6. **huntstop**
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 register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or an MWI.
Step 4	**number** *number*	Associates a phone number with the directory number.

	Command or Action	Purpose
	Example: `Router(config-register-dn)# number 5001`	• Assign the same number to several directory numbers to create a group of virtual dial peers through which the incoming called number must search.
Step 5	**preference** *preference-order* **Example:** `Router(config-register-dn)# preference 4`	Creates the preference order for matching the VoIP dial peers created for the number associated with this directory number to establish the hunt strategy for incoming calls. • Default is 0, which is the highest preference.
Step 6	**huntstop** **Example:** `Router(config-register-dn)# huntstop`	Disables call-hunting behavior for an extension on a SIP phone.
Step 7	**end** **Example:** `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you want to collect statistics for hunt groups, see Cisco Unified CME B-ACD and Tcl Call-Handling Applications.

Enable Call Pickup

To enable Call Pickup features on SCCP or SIP phones, perform the following steps.

Restriction

- SIP phones that do not support the PickUp and GpickUp soft keys must use feature access codes (FACs) to access these features.
- Different directory numbers with the same extension number must have the same Pickup configuration.
- A directory number can be assigned to only one pickup group.
- Pickup group numbers can vary in length, but must have unique leading digits. For example, if you configure group number 17, you cannot also configure group number 177. Otherwise a pickup in group 17 is always triggered before the user can enter the final 7 for 177.
- Calls from H.323 trunks are not supported on SIP phones.

Before You Begin

- SIP phones require Cisco Unified CME 7.1 or a later version.

- The PickUp and GPickUp soft keys display by default on supported SCCP and SIP phones. If previously disabled, you must enable these soft keys with the **softkeys idle** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **service directed-pickup** [**gpickup**]
5. **fac** {**standard** | **custom pickup** {**direct** | **group** | **local**} *custom-fac*}
6. **exit**
7. **ephone-dn** *dn-tag* [**dual-line** | **octo-line**] or **voice register dn** *dn-tag*
8. **pickup-group** *group-number*
9. **pickup-call any-group**
10. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**service directed-pickup** [**gpickup**] **Example:** `Router(config-telephony)# service directed-pickup gpickup`	Enables Directed Call Pickup and modifies the function of the GPickUp and PickUp soft keys. • **gpickup**—(Optional) Enables using the GPickUp soft key to perform Directed Call Pickup on SCCP phones. This keyword is supported in Cisco Unified CME 7.1 and later versions. • This command determines the specific soft keys used to access different Call Pickup features on SCCP and SIP phones. For a description, see the **service directed-pickup** command in the Cisco Unified CME Command Reference.
Step 5	**fac** {**standard** | **custom pickup** {**direct** | **group** | **local**} *custom-fac*}	Enables standard FACs or creates a custom FAC or alias for Pickup features on SCCP and SIP phones.

	Command or Action	Purpose
	Example: `Router(config-telephony)# fac custom pickup group #35`	• **standard—**Enables standard FACs for all phones. Standard FAC for Park Retrieval is **10. • **custom—**Creates a custom FAC for a feature. • *custom-fac*—User-defined code to dial using the keypad on an IP or analog phone. Custom FAC can be up to 256 characters and contain numbers 0 to 9 and * and #.
Step 6	**exit** **Example:** `Router(config-telephony)# exit`	Returns to privileged EXEC mode.

Step 7	**ephone-dn** *dn-tag* [**dual-line** | **octo-line**] or **voice register dn** *dn-tag*
	Example:
	`Router(config)# ephone-dn 20 dual-line`
	or
	`Router(config)# voice register dn 20`
		Enters directory number configuration mode.

Step 8	**pickup-group** *group-number*
	Example:
	`Router(config-ephone-dn)# pickup-group 30`
	or
	`Router(config-register-dn)# pickup-group 30`
		Creates a pickup group and assigns the directory number to the group.
		• *group-number*—String of up to 32 characters. Group numbers can vary in length but must have unique leading digits. For example, if there is a group number 17, there cannot also be a group number 177.
		• This command can also be configured in ephone-dn-template configuration mode and applied to one or more ephone-dns. The ephone-dn configuration has priority over the template configuration.

Step 9	**pickup-call any-group**
	Example:
	`Router(config-ephone-dn)# pickup-call any-group`
	or
	`Router(config-register-dn)# pickup-call any-group`
		Enables a phone user to pickup ringing calls on any extension belonging to a pickup group by pressing the GPickUp soft key and asterisk (*).
		• The ringing extension must be configured with a pickup group using the **pickup-group** command.
		• If this command is not configured, the user can pickup calls in other groups by pressing the GPickUp soft key and dialing the pickup group number.

Step 10	**end**
	Example:
	`Router(config-ephone-dn)# end`
	or
	`Router(config-register-dn)# end`
		Exits configuration mode.

The following example shows the Group Pickup and Local Group Pickup features enabled with the **service directed-pickup gpickup** command. Extension 1005 on phone 5 and extension 1006 on phone 6 are assigned to pickup group 1.

```
telephony-service
load 7960-7940 P00308000500
load E61 SCCP61.8-2-2SR2S
max-ephones 100
max-dn 240
ip source-address 15.7.0.1 port 2000
service directed-pickup gpickup
cnf-file location flash:
cnf-file perphone
voicemail 8900
max-conferences 8 gain -6
call-park system application
transfer-system full-consult
fac standard
create cnf-files version-stamp 7960 Sep 25 2007 21:25:47
!
!
!
ephone-dn 5
number 1005
pickup-group 1
!
!
ephone-dn 6
number 1006
pickup-group 1
!
!
ephone 5
mac-address 0001.2345.6789
type 7962
button 1:5
!
!
!
ephone 6
mac-address 000F.F758.E70E
type 7962
button 1:6
```

Configure Call-Waiting Indicator Tone on SCCP Phone

To specify the type of audible call-waiting indicator on a SCCP phone, perform the following steps. The default is for directory numbers to accept call interruptions, such as call waiting, and to issue a beep tone. Instead of the standard call waiting beep, you can enable a ring tone for call-waiting.

Restriction

- The call-waiting ring option is not supported if the ephone-dn is configured with the **no call-waiting beep accept** command.
- If you configure a button to have a silent ring, you will not hear a call-waiting beep or call-waiting ring regardless of whether the ephone-dn associated with the button is configured to generate a call-waiting beep or call-waiting ring. To configure a button for silent ring, see Assign Directory Numbers to SCCP Phones, on page 260.
- The call-waiting beep volume cannot be adjusted through Cisco Unified CME for the Cisco Unified IP Phone 7902G, Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7912G, Cisco ATA-186, and Cisco ATA-188.
- The call-waiting ring option is not supported on the Cisco Unified IP Phone 7902G, Cisco Unified IP Phone 7905G, or Cisco Unified IP Phone 7912G.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **call-waiting beep** [**accept** | **generate**]
5. **call-waiting ring**
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	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 20 dual-line`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.
Step 4	**call-waiting beep** [**accept** | **generate**] **Example:** `Router(config-ephone-dn)# no call-waiting beep accept`	Enables an ephone-dn to generate or accept call-waiting beeps. • Default is directory number both accepts and generates call-waiting beep. • The beep is heard only if the other ephone-dn is configured to accept call-waiting beeps (default).

	Command or Action	Purpose
Step 5	**call-waiting ring** **Example:** `Router(config-ephone-dn)# call-waiting ring`	(Optional) Enables an ephone-dn to use a ring indicator for call-waiting notification. • To use this command, do not disable call-waiting beep by using the **no call-waiting beep accept** command.
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Verify Call-Waiting Indicator Tone on SCCP Phone

Step 1 Use the **show running-config** command to verify your configuration. Call-waiting settings are listed in the ephone-dn portion of the output. If the **no call-waiting beep generate** and the **no call-waiting beep accept** commands are configured, the **show running-config** command output will display the **no call-waiting beep** command.

Example:

```
Router# show running-config
!
ephone-dn 3 dual-line
 number 126
 name Accounting
 preference 2 secondary 9
 huntstop
 huntstop channel
 call-waiting beep
!
```

Step 2 Use the **show telephony-service ephone-dn** command to display call-waiting configuration information.

Example:

```
Router# show telephony-service ephone-dn

ephone-dn 1 dual-line
 number 126 secondary 1261
 preference 0 secondary 9
 no huntstop
 huntstop channel
 call-forward busy 500 secondary
 call-forward noan 500 timeout 10
 call-waiting beep
```

Configure Cancel Call Waiting on SCCP Phone

To enable a phone user to cancel call waiting by using the CWOff soft key or a FAC, perform the following steps.

Restriction

- Call Waiting must be disabled by pressing the CWOff soft key or using the FAC before placing a call; it cannot be activated or deactivated during a call.
- The CWOff soft key is not available when initiating Call Transfer.

Before You Begin

For information about standard and custom FACs, see Feature Access Codes, on page 757.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **softkeys seized** {[**CallBack**] [**Cfwdall**] [**CWOff**] [**Endcall**] [**Gpickup**] [**HLog**] [**MeetMe**] [**Pickup**] [**Redial**]}
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
8. **exit**
9. **telephony-service**
10. **fac** {**standard** | **custom ccw** *custom-fac*}
11. **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-template** *template-tag* **Example:** `Router(config)# ephone-template 5`	Enters ephone-template configuration mode to create an ephone template.

	Command or Action	Purpose
		• *template-tag*—Unique identifier for the ephone template. Range: 1 to 20.
Step 4	**softkeys seized** {[**CallBack**] [**Cfwdall**] [**CWOff**] [**Endcall**] [**Gpickup**] [**HLog**] [**MeetMe**] [**Pickup**] [**Redial**]} **Example:** `Router(config-ephone-template)# softkeys seized CWOff Cfwdall Endcall Redial`	(Optional) Modifies the order and type of soft keys that display on an IP phone during the seized call state. • You can enter any of the keywords in any order. • Default is all soft keys are displayed in alphabetical order. • Any soft key that is not explicitly defined is disabled.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the ephone template that you created in Step 3, on page 1288.
Step 8	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode.
Step 9	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 10	**fac** {**standard** | **custom ccw** *custom-fac*} **Example:** `Router(config-telephony)# fac custom ccw **8`	Enables standard FACs or creates a custom FAC or alias. • **standard**—Enables standard FACs for all phones. Standard FAC for cancel call waiting is *1. • **custom**—Creates a custom FAC for a FAC type. • *custom-fac*—User-defined code to be dialed using the keypad on an IP or analog phone. Custom FAC can be up to 256 characters long and contain numbers 0 to 9 and * and #.
Step 11	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

The following example shows a configuration where the order of the CWOff soft key is modified for the seized call state in ephone template 5 and assigned to ephone 12. A custom FAC for cancel call waiting is set to **8.

```
telephony-service
 max-ephones 100
 max-dn 240
 voicemail 8900
 max-conferences 8 gain -6
 transfer-system full-consult
 fac custom cancel call waiting **8
!
!
ephone-template  5
 softkeys seized CWOff Cfwdall Endcall Redial
!
!
ephone  12
 ephone-template 5
 mac-address 000F.9054.31BD
 type 7960
 button  1:10 2:7
```

Enable Call Waiting on SIP Phones

To enable call waiting on an individual SIP phone, perform the following steps.

Before You Begin

- Cisco Unified CME 3.4 or a later version.
- **mode cme** command must be configured in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **call-waiting**
5. **exit**
6. **voice register global**
7. **hold-alert** *timeout*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone in Cisco Unified CME.
Step 4	**call-waiting** **Example:** `Router(config-register-pool)# call-waiting`	Configures call waiting on the SIP phone being configured. **Note** This step is included to illustrate how to enable the command if it was previously disabled. • Default: Enabled.
Step 5	**exit** **Example:** `Router(config-register-pool)# exit`	Exits voice register pool configuration mode.
Step 6	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set parameters for all supported SIP phones in Cisco Unified CME.
Step 7	**hold-alert** *timeout* **Example:** `Router(config-register-global)# hold-alert 30`	Sets an audible alert notification when a call is on hold on a SIP phone. Default is disabled. • *timeout*—Interval after which an audible alert notification is repeated, in seconds. Range: 15 to 300.
Step 8	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Configure Ephone-Hunt Groups on SCCP Phones

To define a hunt group and optional agent availability parameters, perform the following steps.

Restriction

- The HLog soft key is available only on display phones. It is not available on Cisco Unified IP Phones 7902, 7905, and 7912; Cisco IP Communicator; and Cisco VG224.
- Shared ephone-dns cannot use the Agent Status Control or Automatic Agent Not-Ready feature.
- If directory numbers that are members of a hunt group are configured for called-name display, the following restrictions apply:
    - The primary or secondary pilot number must be defined using at least one wildcard character.
    - The phone numbers in the **list** command cannot contain wildcard characters.
- If Call Forward All or Call Forward Busy is configured for a hunt group member (directory number), the hunt group ignores it.

Before You Begin

Directory numbers included in a hunt group must be configured in Cisco Unified CME. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-hunt** *hunt-tag* {**longest-idle** | **peer** | **sequential**}
4. **pilot** *number* [**secondary** *number*]
5. **list** *number* [**,** *number...*]
6. **final** *final-number*
7. **hops** *number*
8. **timeout** *seconds* [**,** *seconds...*]
9. **max-timeout** *seconds*
10. **preference** *preference-order* [**secondary** *secondary-order*]
11. **no-reg** [**both** | **pilot**]
12. **fwd-final** {**orig-phone** | **final**}
13. **forward local-calls**
14. **secondary start** [**current** | **next** | *list-position*]
15. **present-call** {**idle-phone** | **onhook-phone**}
16. **from-ring**
17. **description** *text-string*
18. **display-logout** *text-string*
19. **exit**
20. **telephony-service**
21. **max-redirect** *number*
22. **hunt-group logout** {**DND** | **HLog**}
23. **exit**
24. **ephone-dn** *dn-tag*
25. **ephone-hunt login**
26. **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-hunt** *hunt-tag* {**longest-idle** | **peer** | **sequential**}	Enters ephone-hunt configuration mode to define an ephone hunt group.

	Command or Action	Purpose
	Example: `Router(config)# ephone-hunt 23 peer`	• *hunt-tag*—Unique sequence number that identifies this hunt group during configuration tasks. Range: 1 to 100. Cisco CME 3.3 and earlier—Range: 1 to 10 • **longest-idle**—Calls go to the ephone-dn that has been idle the longest for the number of hops specified when the ephone hunt group was defined. The longest-idle is determined from the last time that a phone registered, reregistered, or went on-hook. • **peer**—First ephone-dn to ring is the number to the right of the ephone-dn that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified when the ephone hunt group was defined. • **sequential**—Ephone-dns ring in the left-to-right order in which they are listed when the hunt group is defined.
Step 4	**pilot** *number* [**secondary** *number*] **Example:** `Router(config-ephone-hunt)# pilot 5601`	Defines the pilot number, which is the number that callers dial to reach the hunt group. • *number*—E.164 number up to 27 characters. The dialplan pattern can be applied to the pilot number. • **secondary**—(Optional) Defines an additional pilot number for the ephone hunt group.
Step 5	**list** *number* [**,** *number...*] **Example:** `Router(config-ephone-hunt)# list 5001, 5002, 5017, 5028`	Defines the list of numbers (from 2 and 20) to which the ephone hunt group redirects the incoming calls. • *number*—E.164 number up to 27 characters. Primary or secondary number assigned to an ephone-dn.
Step 6	**final** *final-number* **Example:** `Router(config-ephone-hunt)# final 6000`	Defines the last number in the ephone hunt group, after which the call is no longer redirected. Can be an ephone-dn primary or secondary number, a voice-mail pilot number, a pilot number of another hunt group, or an FXS number. **Note** When a final number is defined as a pilot number of another hunt group, the pilot number of the first hunt group cannot be configured as a final number in any other hunt group. **Note** This command is not used for ephone hunt groups that are part of a Cisco Unified CME B-ACD service. The final destination for those groups is determined by the B-ACD service.
Step 7	**hops** *number* **Example:** `Router(config-ephone-hunt)# hops 7`	(Optional; peer and longest-idle hunt groups only) Sets the number of hops before a call proceeds to the final number. • *number*—Number of hops before the call proceeds to the final ephone-dn. Range is 2 to 20, but the value must be less than or equal to the number of extensions that are specified in the **list** command. Default automatically adjusts to the number of hunt group members.

	Command or Action	Purpose
Step 8	**timeout** *seconds* [**,** *seconds*...] **Example:** `Router(config-ephone-hunt)# timeout 7, 10, 15`	(Optional) Sets the number of seconds after which an unanswered call is redirected to the next number in the hunt-group list. • *seconds*—Number of seconds. Range: 3 to 60000. Multiple entries can be made, separated by commas, that must correspond to the number of ephone-dns in the **list** command. Each number in a multiple entry specifies the time that the corresponding ephone-dn will ring before a call is forwarded to the next number in the list. If a single number is entered, it is used for the no-answer period for each ephone-dn. • If this command is not used, the default is the number of seconds set by the **timeouts ringing** command, which defaults to 180 seconds. Note that the default of 180 seconds may be greater than you desire.
Step 9	**max-timeout** *seconds* **Example:** `Router(config-ephone-hunt)# max-timeout 25`	(Optional) Sets the maximum combined timeout for the no-answer periods for all ephone-dns in the ephone-hunt list. The call proceeds to the final destination when this timeout expires, regardless of whether it has completed the hunt cycle. • *seconds*—Number of seconds. Range is 3 to 60000. • If this command is not used, the default is that no combined timeout limit is set.
Step 10	**preference** *preference-order* [**secondary** *secondary-order*] **Example:** `Router(config-ephone-hunt)# preference 1`	(Optional) Sets a preference order for the ephone-dn associated with the hunt-group pilot number. • *preference-order*—See the CLI help for a range of numeric values, where 0 is the highest preference. Default is 0. • **secondary** *secondary-order*—(Optional) Preference order for the secondary pilot number. See the CLI help for a range of numeric values, where 0 is the highest preference. Default is 7.
Step 11	**no-reg** [**both** | **pilot**] **Example:** `Router(config-ephone-hunt)# no-reg`	(Optional) Prevents the hunt-group pilot number from registering with an H.323 gatekeeper. If this command is not used, the default is that the pilot number registers with the H.323 gatekeeper. • **both**—(Optional) Both the primary and secondary pilot numbers are not registered. • **pilot**—(Optional) Only the primary pilot number is not registered. • In Cisco CME 3.1 and later versions, if this command is used without the either the **both** or **pilot** keywords, only the secondary number is not registered.
Step 12	**fwd-final** {**orig-phone** | **final**} **Example:** `Router(config-ephone-hunt)# fwd-final orig-phone`	(Optional) For calls that have been transferred into an ephone hunt group by a local extension, determines the final destination of a call that is not answered in the hunt group.

	Command or Action	Purpose
		• **final**—Forwards the call to the ephone-dn number that is specified in the **final** command. • **orig-phone**—Forwards the call to the primary directory number of the phone that transferred the call into the hunt group.
Step 13	**forward local-calls** **Example:** `Router(config-ephone-hunt)# no forward local-calls`	(Optional; sequential hunt groups only) Specifies that local calls (calls from ephone-dns on the same Cisco Unified CME system) will not be forwarded past the first list member in a hunt group. If the first member is busy, the internal caller hears busy. If the first number does not answer, the internal caller hears ringback.
Step 14	**secondary start** [**current** | **next** | *list-position*] **Example:** `Router(config-ephone-hunt)# secondary start next`	(Optional) For calls that are parked by hunt group member phones, returns them to a different entry point in the hunt group (as specified in this command) if the calls are recalled from park to the secondary pilot number or transferred from park to an ephone-dn that forwards the call to the secondary pilot number. • **current**—The ephone-dn that parked the call. • **next**—The ephone-dn in the hunt group list that follows the ephone-dn that parked the call. • *list-position*—The ephone-dn at the specified position in the list specified by the **list** command. Range is 1 to 10.
Step 15	**present-call** {**idle-phone** | **onhook-phone**} **Example:** `Router(config-ephone-hunt)# present-call idle-phone`	(Optional) Presents ephone-hunt-group calls only to member phones that are idle or onhook, as specified. • **idle-phone**—A call from the ephone-hunt group is presented to an ephone only if all lines on the phone are idle. This option ignores monitored lines that have been configured on the phone using the **button m** command. • **onhook-phone**—A call from the ephone-hunt group is presented to an ephone only if the phone is in the on-hook state. When this keyword is configured, calls in the ringing or hold state that are unrelated to the hunt group do not prevent the presentation of calls from the ephone-hunt group.
Step 16	**from-ring** **Example:** `Router(config-ephone-hunt)# from-ring`	(Optional) Specifies that on-hook time stamps should be recorded when calls ring extensions and when calls are answered. The default is that on-hook time stamps are recorded only when calls are answered.
Step 17	**description** *text-string* **Example:** `Router(config-ephone-hunt)# description Marketing Hunt Group`	(Optional) Defines text that will appear in configuration output.

	Command or Action	Purpose
Step 18	**display-logout** *text-string* **Example:** `Router(config-ephone-hunt)# display-logout Night Service`	(Optional) Defines text that will appear on IP phones that are members of a hunt group when all the hunt-group members are in the not-ready status. This string can be used to inform hunt-group members where the calls are being sent when all members are unavailable to take calls.
Step 19	**exit** **Example:** `Router(config-ephone-hunt)# exit`	Exits ephone-hunt configuration mode.
Step 20	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 21	**max-redirect** *number* **Example:** `Router(config-telephony)# max-redirect 8`	(Optional) Sets the number of times that a call can be redirected within a Cisco Unified CME system. • *number*—Range is 5 to 20. Default is 10. **Note** This command is required if the number of hops is greater than 10.
Step 22	**hunt-group logout** {**DND** | **HLog**} **Example:** `Router(config-telephony)# hunt-group logout HLog`	(Optional) Specifies whether agent not-ready status applies only to ephone hunt group extensions on a phone (HLog mode) or to all extensions on a phone (DND mode). Agent not-ready status can activated by an agent using the HLog softkey or a FAC, or it can be activated automatically after the number of calls specified in the **auto logout** command are not answered. The default of this command is not used is **DND**. • **DND**—When phones are placed in agent not-ready status, all ephone-dns on the phone will not accept calls. • **HLog**—Enables the display of the HLog soft key. When phones are placed in the agent not-ready status, only the ephone-dns assigned to ephone hunt groups will not accept calls.
Step 23	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 24	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 29`	(Optional) Enters ephone-dn configuration mode. • *dn-tag*—Tag number for the ephone-dn to be authorized to join and leave ephone hunt groups.

	Command or Action	Purpose
Step 25	**ephone-hunt login** **Example:** `Router(config-ephone-dn)# ephone-hunt login`	(Optional) Enables this ephone-dn to join and leave ephone hunt groups (dynamic membership).
Step 26	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Verify Ephone Hunt Groups Configuration

Step 1 Use the **show running-config** command to verify your configuration. Ephone hunt group parameters are listed in the ephone-hunt portion of the output.

Example:

```
Router# show running-config
ephone-hunt 1 longest-idle

pilot 500

list 502, 503, *

max-timeout 30

timeout 10, 10, 10

hops 2

from-ring

fwd-final orig-phone

!

!

ephone-hunt 2 sequential

pilot 600

list 621, *, 623

final 5255348

max-timeout 10

timeout 20, 20, 20

fwd-final orig-phone

!
```

```
!
ephone-hunt 77 longest-idle
from-ring
pilot 100
list 101, *, 102
!
```

Step 2 To verify the configuration of ephone hunt group dynamic membership, use the **show running-config** command. Look at the ephone-hunt portion of the output to ensure at least one wildcard slot is configured. Look at the ephone-dn section to see whether particular ephone-dns are authorized to join ephone hunt groups. Look at the telephony-service section to see whether FACs are enabled.

Example:

```
Router# show running-config
ephone-hunt 1 longest-idle
pilot 500
list 502, 503, *
max-timeout 30
timeout 10, 10, 10
hops 2
from-ring
fwd-final orig-phone
!
!
ephone-dn 2 dual-line
number 126
preference 1
call-forward busy 500
ephone-hunt login
!
telephony-service
fac custom alias 5 *5 to *35000
fac custom ephone-hunt cancel #5
```

Step 3 Use the **show ephone-hunt** command for detailed information about hunt groups, including dial-peer tag numbers, hunt-group agent status, and on-hook time stamps. This command also displays the dial-peer tag numbers of all ephone-dns that have joined dynamically and are members of the group at the time that the command is run.

Example:

```
Router# show ephone-hunt

Group 1
type: peer
pilot number: 450, peer-tag 20123
```

```
list of numbers:
451, aux-number A450A0900, # peers 5, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20122 42 0 login up ]
[20121 41 0 login up ]
[20120 40 0 login up ]
[20119 30 0 login up ]
[20118 29 0 login down]
452, aux-number A450A0901, # peers 4, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20127 45 0 login up ]
[20126 44 0 login up ]
[20125 43 0 login up ]
[20124 31 0 login up ]
453, aux-number A450A0902, # peers 4, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20131 48 0 login up ]
[20130 47 0 login up ]
[20129 46 0 login up ]
[20128 32 0 login up ]
477, aux-number A450A0903, # peers 1, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20132 499 0 login up ]
preference: 0
preference (sec): 7
timeout: 3, 3, 3, 3
max timeout : 10
hops: 4
next-to-pick: 1
E.164 register: yes
auto logout: no
stat collect: no
Group 2
type: sequential
pilot number: 601, peer-tag 20098
list of numbers:
123, aux-number A601A0200, # peers 1, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20097 56 0 login up ]
622, aux-number A601A0201, # peers 3, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20101 112 0 login up ]
[20100 111 0 login up ]
[20099 110 0 login up ]
623, aux-number A601A0202, # peers 3, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20104 122 0 login up ]
[20103 121 0 login up ]
[20102 120 0 login up ]
*, aux-number A601A0203, # peers 1, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20105 0 0 - down]
*, aux-number A601A0204, # peers 1, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20106 0 0 - down]
final number: 5255348
preference: 0
preference (sec): 9
timeout: 5, 5, 5, 5, 5
max timeout : 40
fwd-final: orig-phone
E.164 register: yes
auto logout: no
stat collect: no
Group 3
type: longest-idle
pilot number: 100, peer-tag 20142
list of numbers:
101, aux-number A100A9700, # peers 3, logout 0, down 3
on-hook time stamp 7616, off-hook agents=0
peer-tag dn-tag rna login/logout up/down
```

```
[20141 132 0 login down]
[20140 131 0 login down]
[20139 130 0 login down]
*, aux-number A100A9701, # peers 1, logout 0, down 1
on-hook time stamp 7616, off-hook agents=0
peer-tag dn-tag rna login/logout up/down
[20143 0 0 - down]
102, aux-number A100A9702, # peers 2, logout 0, down 2
on-hook time stamp 7616, off-hook agents=0
peer-tag dn-tag rna login/logout up/down
[20145 142 0 login down]
[20144 141 0 login down]
all agents down!
preference: 0
preference (sec): 7
timeout: 100, 100, 100
hops: 0
E.164 register: yes
auto logout: no
stat collect: no
```

Configure Voice-Hunt Groups

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

Restriction

- Before Cisco Unified CME 4.3, forwarding or transferring to a voice hunt group is not supported.
- In Cisco Unified CME 4.3 and later versions, Call Forwarding is supported to a parallel hunt-group (blast hunt group) only.
- SIP-to-H.323 calls are not supported.
- If Call Forward All or Call Forward Busy is configured for a hunt group member (directory number), the hunt group ignores it.
- Caller ID update is not supported for supplementary services.
- Voice hunt groups are subject to the max-redirect restriction.
- A pilot dial peer cannot be used for a voice hunt group and an ephone hunt group at the same time.
- Voice hunt groups do not support the expansion of pilot numbers using the **dialplan-pattern** command. To enable external phones to dial the pilot number, you must configure a secondary pilot number using a fully qualified E.164 number.
- If call-waiting is enabled (the default), parallel hunt groups support multiple calls up to the limit of call-waiting calls supported by the particular SIP phone model. If call waiting is disabled, parallel hunt groups support only one call at a time in the ringing state. Phones that fail to connect must return to the on-hook state before they can receive other calls.
- A phone number associated with an FXO port is not supported in parallel hunt groups.
- For Unified CME 12.1 and prior releases, mixed shared lines and SIP shared lines are not supported with voice hunt groups.
- If the directory number (member of a voice hunt group) is a shared line, agent status control or HLog is not supported.
- Line level logout or login is not supported using HLog softkey or feature button for SIP phones.
- From Unified CME release 11.6 onwards, line level logout or login is not supported using FAC for SIP phones.
- DND FAC is not supported with SIP phones on Unified CME.
- Consider an SCCP DN that is part of both voice hunt group and ephone hunt group. If voice hunt group is configured with members logout or auto logout, then the SCCP DN will logout only from voice hunt group. If ephone hunt group is configured with members logout or auto logout, then the SCCP DN will logout from both voice hunt group and ephone hunt group.

Before You Begin

- Cisco Unified CME 3.4 or a later version for SIP phones.
- Cisco Unified CME 4.3 or a later version is required to include a SCCP phone, FXS analog phone, DS0-group, PRI-group, or SIP trunk in a voice hunt-group.
- Cisco Unified CME 4.3 or a later version is required for call transfer to a voice hunt-group.
- Directory numbers included in a hunt group must be configured in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.

- Cisco Unified CME 11.6 or later is required to support HLog softkey, feature button, and agent status control.
- Cisco Unified CME 11.6 or later is required to configure **present-call**, **auto logout** , and **members logout** under voice hunt group configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voicehunt-group** *hunt-tag* [**longest-idle** |**parallel** | **peer** | **sequential**]
4. **pilot** *number* [**secondary** *number*]
5. **list** *number*
6. **final** *number*
7. **preference** *preference-order* [**secondary** *secondary-order*]
8. **hops** *number*
9. **timeout** *seconds*
10. **present-call idle-phone**
11. **members logout**
12. **auto logout** *number-of-calls*
13. **exit**
14. **telephony-service**
15. **hunt-group logout** {**DND HLog** }
16. **exit**
17. **voice register dn** *tag*
18. **voice-hunt-groups login**
19. **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	**voicehunt-group** *hunt-tag* [**longest-idle** |**parallel** | **peer** | **sequential**]	Enters voice hunt-group configuration mode to define a hunt group. • *hunt-tag*—Unique sequence number of the hunt group to be configured. Range is 1 to 100.

	Command or Action	Purpose
	Example: `Router(config)# voice hunt-group 1 longest-idle`	• **longest idle—**Hunt group in which calls go to the directory number that has been idle for the longest time. • **sequential—**Hunt group in which directory numbers ring in the order in which they are listed, left to right. • **parallel—**Hunt group in which all directory numbers ring simultaneously. • **peer—**Hunt group in which the call placed to a directory number rings for the next directory number in line. • To change the hunt-group type, remove the existing hunt group first by using the **no** form of the command; then, recreate the group.
Step 4	**pilot** *number* [**secondary** *number*] **Example:** `Router(config-voice-hunt-group)# pilot number 8100`	Defines the telephone number that callers dial to reach a voice hunt group. • *number*—String of up to 16 characters that represents an E.164 telephone number. • Number string may contain alphabetic characters when the number is to be dialed only by the Cisco Unified CME router, as with an intercom number, and not from telephone keypads. • **secondary** *number*—(Optional) Keyword and argument combination defines the number that follows as an additional pilot number for the voice hunt group. • Secondary numbers can contain wild cards. A wildcard is a period (.), which matches any entered digit.
Step 5	**list** *number* **Example:** `Router(config-voice-hunt-group)# list 8000, 8010, 8020, 8030`	Creates a list of extensions that are members of a voice hunt group. To remove a list from a router configuration, use the **no** form of this command. • *number*—List of extensions to be added as members to the voice hunt group. Separate the extensions with commas. • Add or delete all extensions in a hunt-group list at one time. You cannot add or delete a single number in an existing list. • There must be from 2 to 10 extensions in the hunt-group list, and each number must be a primary or secondary number. • Any number in the list cannot be a pilot number of a parallel hunt group.
Step 6	**final** *number* **Example:** `Router(config-voice-hunt-group)# final 8888`	Defines the last extension in a voice hunt group. • If a final number in one hunt group is configured as a pilot number of another hunt group, the pilot number of the first hunt group cannot be configured as a final number in any other hunt group. • This command is not used for voice hunt groups that are part of a Cisco Unified CME B-ACD service. The final destination for those groups is determined by the B-ACD service.

	Command or Action	Purpose
Step 7	**preference** *preference-order* [**secondary** *secondary-order*] **Example:** `Router(config-voice-hunt-group)# preference 6`	Sets the preference order for the directory number associated with a voice hunt-group pilot number. **Note** We recommend that the parallel hunt-group pilot number be unique in the system. Parallel hunt groups may not work if there are more than one partial or exact dial-peer match. For example, if the pilot number is "8000" and there is another dial peer that matches "8…". If multiple matches cannot be avoided, give parallel hunt groups the highest priority to run by assigning a lower preference to the other dial peers. Note that 8 is the lowest preference value. By default, dial peers created by parallel hunt groups have a preference of 0. • *preference-order*—Range is 0 to 8, where 0 is the highest preference and 8 is the lowest preference. Default is 0. • **secondary** *secondary-order*—(Optional) Keyword and argument combination is used to set the preference order for the secondary pilot number. Range is 1 to 8, where 0 is the highest preference and 8 is the lowest preference. Default is 7.
Step 8	**hops** *number* **Example:** `Router(config-voice-hunt-group)# hops 2`	For configuring a peer or longest-idle voice hunt group only. Defines the number of times that a call can hop to the next number in a peer or longest-idle voice hunt group before the call proceeds to the final number. • *number*—Number of hops. Range is 2 to 10, and the value must be less than or equal to the number of extensions specified by the **list** command. • Default is the same number as there are destinations defined under the **list** command.
Step 9	**timeout** *seconds* **Example:** `Router(config-voice-hunt-group)# timeout 100`	Defines the number of seconds after which a call that is not answered is redirected to the next directory number in a voice hunt-group list. • Default: 180 seconds.
Step 10	**present-call idle-phone** **Example:** `Router(config-voice-hunt-group)# present-call idle-phone`	Specifies that voice hunt-group calls are presented only if all lines are idle on the phone on which the hunt-group line appears.
Step 11	**members logout** **Example:** `Router(config-voice-hunt-group)# members logout`	Configures a Cisco Unified CME system for all non-shared static members or agents in a voice hunt group with the Hlogout initial state.
Step 12	**auto logout** *number-of-calls* **Example:** `Router(config-voice-hunt-group)# auto logout 2`	Enables the automatic change of a voice hunt group agent's voice register dn or ephone-dn to not-ready status after a specified number of successive hunt-group calls are not answered.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Router(config-voice-hunt-group)# exit`	Exits voice-hunt-group configuration mode.
Step 14	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 15	**hunt-group logout** {**DND HLog** } **Example:** `Router(config-telephony)# hunt-group logout Hlog`	(Optional) Specifies HLog softkey functions. Agent not-ready status can be activated by an agent using the HLog softkey or a FAC.
Step 16	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 17	**voice register dn** *tag* **Example:** `Router(config)# voice register dn 29`	(Optional) Enters voice register dn configuration mode. • *tag*—Tag number for voice register dn to be authorized to join and leave voice hunt groups.
Step 18	**voice-hunt-groups login** **Example:** `Router(config-register-dn)# voice-hunt-groups login`	(Optional) Enables this voice register dn to join and leave voice hunt groups (dynamic membership).
Step 19	**end** **Example:** `Router(config-register-dn)# end`	Exits to privileged EXEC mode.

Verify Voice Hunt Groups Configuration

Step 1 Use the **show running-config** command to verify your configuration. Voice hunt group parameters are listed in the voice-hunt portion of the output.

Example:

```
Router# show running-config

voice-hunt 1 longest-idle
```

```
pilot 500
list 502, 503, *
max-timeout 30
timeout 10, 10, 10
hops 2
from-ring
fwd-final orig-phone
!
!
voice-hunt 2 sequential
pilot 600
list 621, *, 623
final 5255348
max-timeout 10
timeout 20, 20, 20
fwd-final orig-phone
!
!
voice-hunt 77 longest-idle
from-ring
pilot 100
list 101, *, 102
!
```

Step 2 To verify the configuration of voice hunt group dynamic membership, use the **show running-config** command. Look at the voice-hunt portion of the output to ensure at least one wildcard slot is configured. Look at the voice-dn section to see whether particular ephone-dns are authorized to join voice hunt groups. Look at the telephony-service section to see whether FACs are enabled.

Example:

```
Router# show running-config

voice-hunt 1 longest-idle
pilot 500
list 502, 503, *
max-timeout 30
timeout 10, 10, 10
hops 2
from-ring
fwd-final orig-phone
!
!
voice-dn 2 dual-line
number 126
preference 1
call-forward busy 500
ephone-hunt login
!
telephony-service
fac custom alias 5 *5 to *35000
fac custom ephone-hunt cancel #5
```

Step 3 Use the **show ephone-hunt** command for detailed information about hunt groups, including dial-peer tag numbers, hunt-group agent status, and on-hook time stamps. This command also displays the dial-peer tag numbers of all ephone-dns that have joined dynamically and are members of the group at the time that the command is run.

Example:

```
Router# show ephone-hunt
Group 1
type: peer
pilot number: 450, peer-tag 20123
list of numbers:
451, aux-number A450A0900, # peers 5, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20122 42 0 login up ]
[20121 41 0 login up ]
```

```
[20120 40 0 login up ]
[20119 30 0 login up ]
[20118 29 0 login down]
452, aux-number A450A0901, # peers 4, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20127 45 0 login up ]
[20126 44 0 login up ]
[20125 43 0 login up ]
[20124 31 0 login up ]
453, aux-number A450A0902, # peers 4, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20131 48 0 login up ]
[20130 47 0 login up ]
[20129 46 0 login up ]
[20128 32 0 login up ]
477, aux-number A450A0903, # peers 1, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20132 499 0 login up ]
preference: 0
preference (sec): 7
timeout: 3, 3, 3, 3
max timeout : 10
hops: 4
next-to-pick: 1
E.164 register: yes
auto logout: no
stat collect: no
Group 2
type: sequential
pilot number: 601, peer-tag 20098
list of numbers:
123, aux-number A601A0200, # peers 1, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20097 56 0 login up ]
622, aux-number A601A0201, # peers 3, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20101 112 0 login up ]
[20100 111 0 login up ]
[20099 110 0 login up ]
623, aux-number A601A0202, # peers 3, logout 0, down 0
peer-tag dn-tag rna login/logout up/down
[20104 122 0 login up ]
[20103 121 0 login up ]
[20102 120 0 login up ]
*, aux-number A601A0203, # peers 1, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20105 0 0 - down]
*, aux-number A601A0204, # peers 1, logout 0, down 1
peer-tag dn-tag rna login/logout up/down
[20106 0 0 - down]
final number: 5255348
preference: 0
preference (sec): 9
timeout: 5, 5, 5, 5, 5
max timeout : 40
fwd-final: orig-phone
E.164 register: yes
auto logout: no
stat collect: no
Group 3
type: longest-idle
pilot number: 100, peer-tag 20142
list of numbers:
101, aux-number A100A9700, # peers 3, logout 0, down 3
on-hook time stamp 7616, off-hook agents=0
peer-tag dn-tag rna login/logout up/down
[20141 132 0 login down]
[20140 131 0 login down]
[20139 130 0 login down]
*, aux-number A100A9701, # peers 1, logout 0, down 1
on-hook time stamp 7616, off-hook agents=0
```

```
peer-tag dn-tag rna login/logout up/down
[20143 0 0 - down]
102, aux-number A100A9702, # peers 2, logout 0, down 2
on-hook time stamp 7616, off-hook agents=0
peer-tag dn-tag rna login/logout up/down
[20145 142 0 login down]
[20144 141 0 login down]
all agents down!
preference: 0
preference (sec): 7
timeout: 100, 100, 100
hops: 0
E.164 register: yes
auto logout: no
stat collect: no
```

Enable Audible Tone for Successful Login and Logout of a Hunt Group on SCCP Phone

The user can enable playing of audible tone on an SCCP phone to confirm a successful join or unjoin and login or logout from a hunt group (applies to both ephone and voice hunt group). From Cisco Unified CME 10.5 onwards, distinct audible tone will be played for the following scenarios:

1. To join and unjoin a hunt group via FAC
2. To log in and log out from hunt group via Hlog/DND, or FAC

The audible tone will be played for ephone hunt group and voice hunt group for SCCP Phones.

Restriction

- Supports all 79xx phones except for 7926 wireless phones.

Before You Begin

- Cisco Unified CME 10.5 or a later version
- Ephone or voice hunt group should be configured
- Ephone should be static or dynamic member of hunt group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag* or **ephone-template** *template-tag*
4. **audible tone**
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** *phone-tag* or **ephone-template** *template-tag* **Example:** `Router(config)# ephone 25`	Enters ephone configuration mode. • *phone-tag*—The unique sequence number of the phone that will be notified when an incoming call is received by a night-service ephone-dn during a night-service period. or Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 20.
Step 4	**audible tone** **Example:** `Router(config-ephone)# audible tone`	Enables playing of audible tone on an SCCP phone to confirm a successful login or logout.
Step 5	**end** **Example:** `Router(config-ephone)# end`	

The following example shows that audible tone is configured in voice register pool configuration mode:

```
!
Router(config)# ephone 1
Router(config-ephone)# device-security-mode none
Router(config-ephone)# mac-address 64D8.14A5.C87A
Router(config-ephone)# type 7965
Router(config-ephone)# button 1:3
Router(config-ephone)# audible-tone!
```

Enable the Collection of Call Statistics for Voice Hunt-Groups

To enable the collection of call statistics for voice hunt groups, perform the following steps.

Restriction	Hold and resume statistics are not updated for remote SCCP voice hunt group agents.

Before You Begin

Cisco Unified CME 9.0 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice hunt-group** *hunt-tag* {**longest-idle** \| **parallel** \| **peer** \| **sequential**}
4. **statistics collect**
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 hunt-group** *hunt-tag* {**longest-idle** | **parallel** | **peer** | **sequential**} **Example:** `Router(config)# voice hunt-group 60 longest-idle`	Enters voice hunt-group configuration mode. • *hunt-tag*—Unique sequence number that identifies the hunt group. Range: 1 to 100. • **longest-idle**—Hunt group in which calls go to the directory number that has been idle the longest. • **parallel**—Hunt group in which calls simultaneously ring multiple phones. • **peer**—Hunt group in which the first extension to ring is selected round-robin from the list. Ringing proceeds in a circular manner, left to right, for the number of hops specified when the hunt group is defined. The round-robin selection starts with the number left of the number that answered when the hunt-group was last called. • **sequential**—Hunt group in which extensions ring in the order in which they are listed, left to right, when the hunt group was defined.

	Command or Action	Purpose
Step 4	**statistics collect** **Example:** `Router(config-voice-hunt-group)# statistics collect`	Enables the collection of call statistics for a voice hunt group.
Step 5	**end** **Example:** `Router(config-voice-hunt-group)# end`	Exits to privileged EXEC mode.

Associate a Name with a Called Voice Hunt-Group

Restriction Cisco Unified SIP IP phones are not supported. The display support applies to Cisco Unified SCCP IP phones on voice hunt-group and ephone-hunt configuration modes only.

Before You Begin

Cisco Unified CME 9.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice hunt-group** *hunt-tag* {**parallel**}
4. **final** *number*
5. **list** *number* [, *number...*]
6. **timeout** *seconds*
7. **pilot** *number* [**secondary** *number*]
8. **name** "*primary pilot name*" [**secondary** "*secondary pilot name*"]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice hunt-group** *hunt-tag* {**parallel**} **Example:** `Router(config)# voice hunt-group 20 parallel`	Creates a hunt group for phones in a Cisco Unified CME system. • *hunt-tag*—Unique sequence number that identifies the hunt group. Range is 1 to 100. • **parallel**—Hunt group in which calls simultaneously ring multiple phones.
Step 4	**final** *number* **Example:** `Router(config-voice-hunt-group)# final 4000`	Defines the last extension in a voice hunt group. • *number*—Telephone or extension number. Can be an E.164 number, voice-mail number, pilot number of another hunt group, or FXS caller-ID number.
Step 5	**list** *number* [, *number...*] **Example:** `Router(config-voice-hunt-group)# list 3001, 3002, 3003`	Defines a list of extensions that are members of a voice hunt group. • *number*—Extension or E.164 number assigned to a phone in Cisco Unified CME. List must contain 2 to 32 numbers.
Step 6	**timeout** *seconds* **Example:** `Router(config-voice-hunt-group)# timeout 20`	Defines the number of seconds after which a call that is not answered is redirected to the next number in a voice hunt-group list. • *seconds*—Number of seconds. Range is 3 to 60000. Default is 180.
Step 7	**pilot** *number* [**secondary** *number*] **Example:** `Router(config-voice-hunt-group)# pilot 4045550110 secondary 3125550120`	Defines the number that callers dial to reach a Cisco Unified CME voice hunt group. • *number*—String of up to 32 characters that represents an extension or E.164 telephone number. • **secondary** *number*—(Optional) Defines an additional pilot number for the voice hunt group.
Step 8	**name** "*primary pilot name*" [**secondary** "*secondary pilot name*"] **Example:** `Router(config-voice-hunt-group)# name Hospital secondary "Health Center"`	Associates a name with the called voice hunt group. • "*primary pilot name*"—Name for the primary pilot number. • **secondary** "*secondary pilot name*"—(Optional) Name for the secondary pilot number. **Note** Use quotes (") when input strings have spaces in between.

Prevent Local Call Forwarding to Final Agent in Voice Hunt-Groups

Before You Begin

Cisco Unified CME 9.5 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice hunt-group** *hunt-tag* {**parallel** | **sequential**}
4. [**no**] **forward local-calls to-final**

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 hunt-group** *hunt-tag* {**parallel** | **sequential**} **Example:** `Router(config)# voice hunt-group 1 sequential`	Creates a hunt group for phones in a Cisco Unified CME system. • *hunt-tag*—Unique sequence number that identifies the hunt group. Range is 1 to 100. • **parallel**—Hunt group in which calls simultaneously ring multiple phones. • **sequential**—Hunt group in which extensions ring in the order in which they are listed, left to right, when the hunt group was defined.
Step 4	[**no**] **forward local-calls to-final** **Example:** `Router(config-voice-hunt-group)# no forward local-calls to-final`	Prevents local calls from being forwarded to the final destination number.

Configure Night Service on SCCP Phones

This procedure defines night-service hours, an optional night-service code, the ephone-dns that trigger the notification process, and the ephones that will receive notification.

Restriction

- Night service notification is not supported on analog endpoints connected to FXS ports on a Cisco Integrated Services Router (ISR) or Cisco VG224 Analog Phone Gateway.
- In Cisco Unified CME 4.0 and later versions, silent ringing, configured on the phone by using the **s** keyword with the **button** command, is suppressed when used with the night service feature. Silent ringing is overridden and the phone audibly rings during designated night-service periods.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **night-service day** *day start-time stop-time*
5. **night-service date** *month date start-time stop-time*
6. **night-service everyday** *start-time stop-time*
7. **night-service weekday** *start-time stop-time*
8. **night-service weekend** *start-time stop-time*
9. **night-service code** *digit-string*
10. **timeouts night-service-bell** *seconds*
11. **exit**
12. **ephone-dn** *dn-tag*
13. **night-service bell**
14. **exit**
15. **ephone** *phone-tag*
16. **night-service bell**
17. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**night-service day** *day start-time stop-time* **Example:** `Router(config-telephony)# night-service day mon 19:00 07:00`	Defines a recurring time period associated with a day of the week during which night service is active. • *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 night service, 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 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 5	**night-service date** *month date start-time stop-time* **Example:** `Router(config-telephony)# night-service date jan 1 00:00 00:00`	Defines a recurring time period associated with a month and date during which night service is active. • *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 1 to 31. • *start-time stop-time*—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. The stop time must be greater than the start time. The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.
Step 6	**night-service everyday** *start-time stop-time* **Example:** `Router(config-telephony)# night-service everyday 1200 1300`	Defines a recurring night-service time period to be effective everyday. • *start-time stop-time*—Beginning and ending times for night service, 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 the day following the start time. For example, "19:00 07:00" means "from 7 p.m. to 7 a.m. the next morning." The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
Step 7	**night-service weekday** *start-time stop-time*	Defines a recurring night-service time period to be effective on all weekdays.

	Command or Action	Purpose
	Example: `Router(config-telephony)# night-service weekday 1700 0700`	• *start-time stop-time*—Beginning and ending times for night service, 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 the day following the start time. For example, "19:00 07:00" means "from 7 p.m. to 7 a.m. the next morning." The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
Step 8	**night-service weekend** *start-time stop-time* **Example:** `Router(config-telephony)# night-service weekend 00:00 00:00`	Defines a recurring night-service time period to be effective on all weekend days (Saturday and Sunday). • *start-time stop-time*—Beginning and ending times for night service, 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 the day following the start time. For example, "19:00 07:00" means "from 7 p.m. to 7 a.m. the next morning." The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
Step 9	**night-service code** *digit-string* **Example:** `Router(config-telephony)# night-service code *6483`	Designates a code that can be dialed from any night-service line (ephone-dn) to toggle night service on and off for all lines assigned to night service in the system. • *digit-string*—String of up to 16 keypad digits. The code must begin with an asterisk (*).
Step 10	**timeouts night-service-bell** *seconds* **Example:** `Router(config-telephony)# timeouts night-service-bell 15`	Defines the frequency of the night-service notification. • *seconds*—Range: 4 to 30. Default: 12.
Step 11	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 12	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 55`	Enters ephone-dn configuration mode to define an ephone-dn to receive night-service treatment.
Step 13	**night-service bell** **Example:** `Router(config-ephone-dn)# night-service bell`	Marks this ephone-dn for night-service treatment.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 15	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. • *phone-tag*—The unique sequence number of the phone that will be notified when an incoming call is received by a night-service ephone-dn during a night-service period.
Step 16	**night-service bell** **Example:** `Router(config-ephone)# night-service bell`	Marks this phone to receive night-service bell notification when incoming calls are received on ephone-dns marked for night service during the night-service time period. • Night service notification is not supported on analog endpoints connected to SCCP FXS ports on a Cisco ISR or Cisco VG224.
Step 17	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Configure Night Service on SIP Phones

This procedure defines night-service hours, an optional night-service code, the voice register DNs that trigger the notification process, and the SIP phones (voice register pools) that receive notification. The CLI commands related to night-service in telephony-service are used to make night service feature work on SIP phones.

Restriction

- When **service directed-pickup gpickup** is configured under telephony service, gpickup softkey has to be used on SCCP phones to pick up the ringing call on night-service extensions.

Before You Begin

- It is mandatory to configure the CLI command **service directed-pickup gpickup** under telephony-service to pick up calls from SIP phones for night service.
- It is mandatory to configure source IP address, port, and max dn under telephony-service configuration to make night service feature work for SIP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **night-service day** *day start-time stop-time*
5. **night-service date** *month date start-time stop-time*
6. **night-service everyday** *start-time stop-time*
7. **night-service weekday** *start-time stop-time*
8. **night-service weekend** *start-time stop-time*
9. **fac standard**
10. **night-service code** *digit-string*
11. **timeouts night-service-bell** *seconds*
12. **exit**
13. **voice register dn** *dn-tag*
14. **night-service bell**
15. **exit**
16. **voice register pool** *pool -tag* | **voice register template** *template-tag*
17. **night-service bell**
18. **voice register pool** *pool-tag*
19. **template** *template-tag*
20. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**night-service day** *day start-time stop-time* **Example:** `Router(config-telephony)# night-service day mon 19:00 07:00`	Defines a recurring time period associated with a day of the week during which night service is active. • *day*—Day of the week abbreviation. The following are valid day abbreviations: **sun**, **mon**, **tue**, **wed**,**thu**, **fri**, **sat**.

	Command or Action	Purpose
		• *start-time stop-time*—Beginning and ending times for night service, 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 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 5	**night-service date** *month date start-time stop-time* **Example:** `Router(config-telephony)# night-service date jan 1 00:00 00:00`	Defines a recurring time period associated with a month and date during which night service is active. • *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 1 to 31. • *start-time stop-time*—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. The stop time must be greater than the start time. The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.
Step 6	**night-service everyday** *start-time stop-time* **Example:** `Router(config-telephony)# night-service everyday 1200 1300`	Defines a recurring night-service time period to be effective everyday. • *start-time stop-time*—Beginning and ending times for night service, 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 the day following the start time. For example, "19:00 07:00" means "from 7 p.m. to 7 a.m. the next morning." The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
Step 7	**night-service weekday** *start-time stop-time* **Example:** `Router(config-telephony)# night-service weekday 1700 0700`	Defines a recurring night-service time period to be effective on all weekdays. • *start-time stop-time*—Beginning and ending times for night service, 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 the day following the start time. For example, "19:00 07:00" means "from 7 p.m. to 7 a.m. the next morning." The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
Step 8	**night-service weekend** *start-time stop-time* **Example:** `Router(config-telephony)# night-service weekend 00:00 00:00`	Defines a recurring night-service time period to be effective on all weekend days (Saturday and Sunday). • *start-time stop-time*—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. If the stop time is a

	Command or Action	Purpose
		smaller value than the start time, the stop time occurs the day following the start time. For example, "19:00 07:00" means "from 7 p.m. to 7 a.m. the next morning." The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
Step 9	**fac standard** **Example:** `Router(config-telephony)# fac standard`	(Optional) Enables predefined standard feature access codes (FACs) to be enabled. For the CLI command **night-service code** to work, it is mandatory to configure **fac standard** under **telephony-service** configuration mode.
Step 10	**night-service code** *digit-string* **Example:** `Router(config-telephony)# night-service code *6483`	Designates a code that can be dialed from any night-service line (voice register dn) to toggle night service on and off for all lines assigned to night service in the system. • *digit-string*—String of up to 16 keypad digits. The code must begin with an asterisk (*).
Step 11	**timeouts night-service-bell** *seconds* **Example:** `Router(config-telephony)# timeouts night-service-bell 15`	Defines the frequency of the night-service notification. • *seconds*—Range: 4 to 30. Default: 12.
Step 12	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 13	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 10`	Enters voice register dn configuration mode to define a voice register dn to receive night-service treatment.
Step 14	**night-service bell** **Example:** `Router(config-register-dn)# night-service bell`	Marks this voice register dn for night-service treatment.
Step 15	**exit** **Example:** `Router(config-register-dn)# exit`	Exits voice register dn configuration mode.
Step 16	**voice register pool** *pool -tag* | **voice register template** *template-tag*	Enters pool configuration mode (or template configuration mode). • *pool-tag*—The unique sequence number of the phone that will be notified when an incoming call is received by a night-service voice-dn during a night-service period.

	Command or Action	Purpose

	Example:
	`Router(config)# voice register pool 10`
	
	`Router(config)# voice register template 1`	

Step 17	**night-service bell**
	
	Example:
	`Router(config-register-pool)# night-service bell`
	`Router(config-register-template)# night-service bell`
		Marks this phone to receive night-service bell notification when incoming calls are received on voice register dns marked for night service during the night-service time period.

Step 18	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 10`	Enters pool configuration mode. This step is valid only when the night service configuration is under voice register template.
Step 19	**template** *template-tag* **Example:** `Router(config-register-pool)# template 1`	Includes the template with night-service bell configured to provide night service treatment for this pool. This step is valid only when the night service configuration is under voice register template.
Step 20	**end** **Example:** `Router(config-register-temp)# end`	Returns to privileged EXEC mode.

Verify Night Service Configuration on SCCP Phones

Step 1 Use the **show running-config** command to verify the night-service parameters, which are listed in the telephony-service portion of the output, or use the **show telephony-service** command to display the same parameters.

Example:

Router# **show running-config**

```
telephony-service
 fxo hook-flash
 load 7910 P00403020214
 load 7960-7940 P00303020214
 max-ephones 48
 max-dn 288
 ip source-address 10.50.50.1 port 2000
 application segway0
 caller-id block code *321
 create cnf-files version-stamp 7960 Mar 07 2003 11:19:18
 voicemail 79000
 max-conferences 8
 call-forward pattern .....
 moh minuet.wav
 date-format yy-mm-dd
 transfer-system full-consult
 transfer-pattern .....
 secondary-dialtone 9
 night-service code *1234
 night-service day Tue 00:00 23:00
 night-service day Wed 01:00 23:59
!
!
```

Router# **show telephony-service**

```
CONFIG (Version=4.0(0))
=====================
Version 4.0(0)
Cisco Unified CallManager Express
For on-line documentation please see:
www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

ip source-address 10.103.3.201 port 2000
load 7910 P00403020214
load 7961 TERM41.7-0-1-1
load 7961GE TERM41.7-0-1-1
load 7960-7940 P00307020300
max-ephones 100
max-dn 500
max-conferences 8 gain -6
dspfarm units 2
dspfarm transcode sessions 4
dspfarm 1 MTP00059a3d7441
dspfarm 2
```

```
hunt-group report delay 1 hours
Number of hunt-group configured: 14
hunt-group logout DND
max-redirect 20
voicemail 7189
cnf-file location: system:
cnf-file option: PER-PHONE-TYPE
network-locale[0] US   (This is the default network locale for this box)
user-locale[0] US    (This is the default user locale for this box)
moh flash:music-on-hold.au
time-format 12
date-format mm-dd-yy
timezone 0 Greenwich Standard Time
secondary-dialtone 9
call-forward pattern .T
transfer-pattern 92......
transfer-pattern 91..........
transfer-pattern .T
after-hours block pattern 1 91900 7-24
after-hours block pattern 2 9976 7-24
after-hours block pattern 4 91...976.... 7-24
night-service time is activated
night-service date Jan 1 00:00 23:59
night-service day Mon 17:00 07:00
night-service day Wed 17:00 07:00
keepalive 30
timeout interdigit 10
timeout busy 10
timeout ringing 100
caller-id name-only: enable
system message XYZ Company
web admin system name xyz password xxxx
web admin customer name Customer

edit DN through Web:  enabled.
edit TIME through web:  enabled.
Log (table parameters):
     max-size: 150
     retain-timer: 15
create cnf-files version-stamp Jan 01 2002 00:00:00
transfer-system full-consult

multicast moh 239.10.10.1 port 2000
fxo hook-flash
local directory service: enabled.
```

Step 2 Use the **show running-config** command to verify that the correct ephone-dns and ephones are configured with the **night-service bell** command. You can also use the **show telephony-service ephone-dn** and **show telephony-service ephone** commands to display these parameters.

Example:

Router# **show running-config**

```
ephone-dn 24 dual-line
 number 2548
 description FrontDesk
 night-service bell


ephone  1
 mac-address 110F.80C0.FE0B
 type 7960 addon 1 7914
 no dnd feature-ring
 keep-conference
 button  1f40 2f41 3f42 4:30
 button  7m20 8m21 9m22 10m23
 button  11m24 12m25 13m26
 night-service bell
```

Verify Night Service Configuration on SIP Phones

Step 1 Use the **show running-config | section telephony-service** command to verify the night-service parameters that are listed in the telephony-service portion of the output. Use the **show telephony-service** command to display the same parameters.

Example:

Router# **show running-config | section telephony-service**

```
telephony-service
 max-ephones 50
 max-dn 50
 ip source-address 10.50.50.1 port 2000
 service phone sshAccess 0
 service phone webAccess 0
 service directed-pickup gpickup
 time-zone 39
 max-conferences 8 gain -6
 call-park system application
 hunt-group report url suffix 0 to 100
 hunt-group report every 1 hours
 hunt-group logout HLog
 transfer-system full-consult
 night-service weekday 13:17 14:17
 night-service day Sun 00:05 23:59
 night-service day Sat 00:05 23:59
```

Router# **show telephony-service**

```
max-ephones 50
 max-dn 50
 ip source-address 10.50.50.1 port 2000
 service phone sshAccess 0
 service phone webAccess 0
 service directed-pickup gpickup
 time-zone 39
 max-conferences 8 gain -6
```

```
 call-park system application
 hunt-group report url suffix 0 to 100
 hunt-group report every 1 hours
 hunt-group logout HLog
 transfer-system full-consult
 night-service time is activated
 night-service weekday 13:17 14:17
 night-service day Sun 00:05 23:59
 night-service day Sat 00:05 23:59
```

Step 2 Use the **show voice register dn** and **show voice register pool** command to verify that the correct voice register dns and phones are configured with the **night-service bell** command.

Example:

```
Router# show voice register dn 1

Dn Tag 1
Config:
 Number is 8001
 Preference is 0
 Huntstop is disabled
 Auto answer is disabled
 Pickup group is 5
 Night Service Bell is enabled

Router# show voice register pool 5

 Pool Tag 5
Config:
 Mac address is B000.B4BE.F32C
 Type is 8851
 Number list 1 : DN 5
 Proxy Ip address is 0.0.0.0
 DTMF Relay is disabled
 Call Waiting is enabled
 DnD is disabled
 Video is disabled
 Camera is disabled
 Night Service Bell is enabled
 Busy trigger per button value is 2
```

Configure Overlaid Ephone-dns on SCCP Phones

To create ephone-dns, then assign multiple ephone-dns to a single phone button by using the **o** or **c** keyword with the **button** command, perform the following steps.

Restriction

- Call waiting is disabled when you configure ephone-dn overlays using the **o** keyword with the **button** command. To enable call waiting, you must configure ephone-dn overlays using the **c** keyword with the **button** command.
- Rollover of overlay calls to another phone button by using the **x** keyword with the **button** command only works to expand coverage if the overlay button is configured with the **o** keyword in the **button** command. Overlay buttons with call waiting that use the **c** keyword in the **button** command are not eligible for overlay rollover.
- In Cisco Unified CME 4.0(3), the Cisco Unified IP Phone 7931G cannot support overlays that contain ephone-dn configured for dual-line mode.
- The primary ephone-dn on each phone in a shared-line overlay set should be an ephone-dn that is unique to the phone to guarantee that the phone will have a line available for outgoing calls, and to ensure that the phone user can obtain dial-tone even when there are no idle lines available in the rest of the shared-line overlay set. Use a unique ephone-dn in this manner to provide for a unique calling party identity on outbound calls made by the phone so that the called user can see which specific phone is calling.
- Octo-line directory numbers are not supported in button overlay sets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *phone-tag* [**dual-line**]
4. **number** *number*
5. **preference** *preference-order*
6. **no huntstop** or **huntstop**
7. **huntstop channel**
8. **call-forward noan**
9. **call-forward busy**
10. **exit**
11. **ephone** *phone-tag*
12. **mac-address** *mac-address*
13. **button** *button-number* {**o** | **c**}*dn-tag*, *dn-tag* [, *dn-tag*...] *button-number* {**x**} *overlay-button-number*
14. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-dn** *phone-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 10 dual-line`	Enters ephone-dn configuration mode to create an extension (ephone-dn) for a Cisco Unified IP phone line. • For shared-line overlay set: Primary ephone-dn on a phone should be an ephone-dn that is unique to the phone.
Step 4	**number** *number* **Example:** `Router(config-ephone-dn)# number 1001`	Associates a telephone or extension number with the ephone-dn.
Step 5	**preference** *preference-order* **Example:** `Router(config-ephone-dn)# preference 1`	Sets dial-peer preference order for an ephone-dn. • *preference-order*—Preference order for the primary number associated with an extension (ephone-dn). Type **?** for a range of numeric options, where 0 is the highest preference. Default: 0.

Step 6	**no huntstop** or **huntstop**
	
	Example:
	`Router(config-ephone-dn)# no huntstop`
	`or`
	`Router(config-ephone-dn)# huntstop`
		Explicitly enables call hunting behavior for a directory number.
		• Set this command on all ephone-dns in the overlay set except the final instance.
		• Required to allow call hunting allow call hunting across multiple numbers on the same line button on an IP phone.
		
		or
		
		Disables call hunting behavior for a directory number.
		• Set this command on the last ephone-dn within a overlay set.
		• Required to limit the call hunting to an overlay set.

Step 7	**huntstop channel** **Example:** `Router(config-ephone-dn)# huntstop channel`	Only for dual-line ephone-dns in overlay set; keeps incoming calls from hunting to the second channel if the first channel is busy or does not answer. • Reserves the second channel for outgoing calls, such as a consultation call to be placed during a call transfer attempt, or for conferencing
Step 8	**call-forward noan** **Example:** `Router(config-ephone-dn)# call-forward noan`	(Optional) Forwards incoming unanswered call to next line in the overlay set. • Set this command on all ephone-dns in the overlay set.
Step 9	**call-forward busy**	(Optional) Forwards incoming call if line is busy.

	Command or Action	Purpose
	Example: `Router(config-ephone-dn)# call-forward busy`	• Set this command on the last ephone-dn in the overlay set only.
Step 10	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode
Step 11	**ephone** *phone-tag* **Example:** `Router(config)# ephone 4`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies the phone to which you are adding an overlay set.
Step 12	**mac-address** *mac-address* **Example:** `Router(config-ephone)# mac-address 1234.5678.abcd`	Specifies the MAC address of the registering phone.
Step 13	**button** *button-number* {**o** | **c**}*dn-tag*, *dn-tag* [, *dn-tag*...] *button-number* {**x**} *overlay-button-number* **Example:** `Router(config-ephone)# button 1o15,16,17,18,19 2c20,21,22 3x1 4x1`	Creates a set of ephone-dns overlaid on a single button. • **o**—Overlay button. Multiple ephone-dns share this button. A maximum of 25 ephone-dns can be specified for a single button, separated by commas. • **c**—Overlay button with call-waiting. Multiple ephone-dns share this button. A maximum of 25 ephone-dns can be specified for a single button, separated by commas. • **x**—Separator that creates a rollover button for an overlay button that was defined using the **o** keyword. When the overlay button specified in this command is occupied by an active call, a second call to one of its ephone-dns will be presented on this button. • *dn-tag*—Unique identifier previously defined with the **ephone-dn** command for the ephone-dn to be added to this overlay set. • *overlay-button-number*—Number of the overlay button that should overflow to this button. Note that the button must have been defined using the **o** keyword and not the **c** keyword. **Note** For other keywords, see the **button** command in the Cisco Unified Communications Manager Express Command Reference.
Step 14	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verify Overlaid Ephone-dns Configuration on SCCP Phone

Step 1 Use the **show running-config** command or the **show telephony-service ephone** command to view button assignments.

```
Router# show running-config

ephone  5
 description Cashier1
 mac-address 0117.FBC6.1985
 type 7960
 button  1o4,5,6,200,201,202,203,204,205,206 2x1 3x1
```

Step 2 Use the **show ephone overlay** command to display the configuration and current status of registered overlay ephone-dns.

Step 3 Use the **show dialplan number** command to display all the number resolutions of a particular phone number, which allows you to detect whether calls are going to unexpected destinations. This command is useful for troubleshooting cases in which you dial a number but the expected phone does not ring.

Enable Out-Of-Dialog REFER

Restriction

- The call waiting, conferencing, hold, and transfer call features are not supported while the Refer-Target is ringing.
- In a SIP to SIP scenario, no ringback is heard by the Referee when Refer-Target is ringing.

Before You Begin

- Cisco Unified CME 4.1 or a later version.
- The application that initiates OOD-R, such as a click-to-dial application, and its directory server must be installed and configured.
- For information on the SIP REFER and NOTIFY methods used between the directory server and Cisco Unified CME, see RFC 3515, The Session Initiation Protocol (SIP) Refer Method.
- For information on the message flow Cisco Unified CME uses when initiating a session between the Referee and Refer-Target, see RFC 3725, Best Current Practices for Third Party Call Control (3pcc).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **refer-ood enable** [*request-limit*]
5. **exit**
6. **voice register global**
7. **authenticate ood-refer**
8. **authenticate credential** *tag location*
9. **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	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode to configure the user agent.
Step 4	**refer-ood enable** [*request-limit*] **Example:** `Router(config-sip-ua)# refer-ood enable 300`	Enables OOD-R processing. • *request-limit*—Maximum number of concurrent incoming OOD-R requests that the router can process. Range: 1 to 500. Default: 500.
Step 5	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits SIP user-agent configuration mode.
Step 6	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode to set global parameters for all supported SIP phones in a Cisco Unified CME or Cisco Unified SRST environment.

	Command or Action	Purpose
Step 7	**authenticate ood-refer** **Example:** `Router(config-register-global)# authenticate ood-refer`	(Optional) Enables authentication of incoming OOD-R requests using RFC 2617-based digest authentication.
Step 8	**authenticate credential** *tag location* **Example:** `Router(config-register-global)# authenticate credential 1 flash:cred1.csv`	(Optional) Specifies the credential file to use for authenticating incoming OOD-R requests. • *tag*—Number that identifies the credential file to use for OOD-R authentication. Range: 1 to 5. • *location*—Name and location of the credential file in URL format. Valid storage locations are TFTP, HTTP, and flash memory.
Step 9	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

What to Do Next

- If you are configuring Cisco Unified CME for the first time on this router, you are ready to configure system-level parameters. See Configure System-Level Parameters, on page 167.
- If you modified network parameters for an already configured Cisco Unified CME router, you are ready to generate the configuration file to save the modifications. See Generate Configuration Files for Phones, on page 388.

Verify OOD-R Configuration

SUMMARY STEPS

1. **show running-config**
2. **show sip-ua status refer-ood**

DETAILED STEPS

Step 1 **show running-config**

This command verifies your configuration.

Example:

```
Router# show running-config
```

```
!
voice register global
mode cme
source-address 10.1.1.2 port 5060
load 7971 SIP70.8-0-1-11S
load 7970 SIP70.8-0-1-11S
load 7961GE SIP41.8-0-1-0DEV
load 7961 SIP41.8-0-1-0DEV
authenticate ood-refer
authenticate credential 1 tftp://172.18.207.15/labtest/cred1.csv
create profile sync 0004550081249644
.
.
.
sip-ua
refer-ood enable
```

Step 2 **show sip-ua status refer-ood**
This command displays OOD-R configuration settings.

Example:

```
Router# show sip-ua status refer-ood

Maximum allow incoming out-of-dialog refer 500
Current existing incoming out-of-dialog refer dialogs: 1
outgoing out-of-dialog refer dialogs: 0
```

Troubleshooting OOD-R

Step 1 Use the **debug ccsip messages** command to display the SIP messages exchanged between the SIP UA client and the router.

Step 2 Use the **debug voip application oodrefer** command to display debugging messages for the OOD-R feature.

Configuration Examples for Call Coverage Features

Call Hunt: Examples

Example for Setting Ephone-dn Dial-Peer Preference

The following example sets a preference number of 2 for the primary number of ephone-dn 3:

```
ephone-dn 3
 number 3001
 preference 2
```

Example for Disabling Huntstop

The following example shows an instance in which huntstop is not desired and is explicitly disabled. In this example, ephone 4 is configured with two lines, each with the same extension number 5001. This is done to allow the second line to provide call waiting notification for extension number 5001 when the first line is in use. Setting **no huntstop** on the first line (ephone-dn 1) allows incoming calls to hunt to the second line (ephone-dn 2) on the same phone when the ephone-dn 1 line is busy.

Ephone-dn 2 has call forwarding set to extension 6000, which corresponds to a locally attached answering machine connected to a foreign exchange station (FXS) voice port. The plain old telephone service (POTS) dial peer for extension 6000 also has the dial-peer huntstop attribute explicitly set to prevent further hunting.

```
ephone-dn 1
 number 5001
 no huntstop
 preference 1
 call-forward noan 6000

ephone-dn 2
 number 5001
 preference 2
 call-forward busy 6000
 call-forward noan 6000

ephone 4
 button 1:1 2:2
 mac-address 0030.94c3.8724
 dial-peer voice 6000 pots
 destination-pattern 6000
 huntstop port 1/0/0
 description answering-machine
```

Example for Channel Huntstop

The following is an example that uses the **huntstop channel** command. It shows a dual-line ephone-dn configuration in which calls do not hunt to the second channel of any ephone-dn, but they do hunt through each ephone-dn's channel 1 in this order: ephone-dn 10, ephone-dn 11, ephone-dn 12.

```
ephone-dn 10 dual-line
 number 1001
 no huntstop
 huntstop channel

ephone-dn 11 dual-line
 number 1001
 no huntstop
 huntstop channel
 preference 1

ephone-dn 12 dual-line
 number 1001
 no huntstop
 huntstop channel
 preference 2
```

Example for SIP Call Hunt

The following example shows a typical configuration in which huntstop is required. The **huntstop** command is enabled and prevents calls to extension 5001 from being rerouted to the on-net H.323 dial peer for 5... when extension 5001 is busy (three periods are used as wild cards).

```
voice register dn 1
 number 5001
 huntstop

voice register pool 4
 number 1 dn 1
 id-mac 0030.94c3.8724

dial-peer voice 5000 voip
 destination-pattern 5...
 session target ipv4:192.168.17.225
 session protocol sipv2
```

Example for Call Pickup

The following example assigns the line that has an ephone-dn tag of 55 to pickup group 2345:

```
ephone-dn 55
 number 2555
 pickup-group 2345
```

The following example globally disables directed call pickup and changes the action of the PickUp soft key to perform local group call pickup rather than directed call pickup:

```
telephony-service
 no service directed-pickup
```

Example for Call-Waiting Beep

In the following example, ephone-dn 10 neither accepts nor generates a beep, ephone-dn 11 does not accept a beep, and ephone-dn 12 does not generate a beep:

```
ephone-dn 10
 no call-waiting beep
 number 4410

ephone-dn 11
 no call-waiting beep accept
 number 4411

ephone-dn 12
 no call-waiting beep generate
 number 4412
```

Example for Call-Waiting Ring

The following example specifies that a short ring will indicate a call is waiting for extension 5533:

```
ephone-dn 20
```

```
 number 5533
 call-waiting ring
```

Examples for Hunt Group

Example for Sequential Ephone-Hunt Group

The following example defines a sequential ephone hunt group with the pilot number 5600 and the final number 6000, with three numbers in the list of phones that answer for the pilot number:

```
ephone-hunt 2 sequential
 pilot 5600
 list 5621, *, 5623
 final 6000
 max-timeout 10
 timeout 20, 20, 20
 fwd-final  orig-phone
```

Example for Peer Ephone-Hunt Group

The following example defines peer ephone hunt group 10 with a pilot number 450, a final number 500, and four numbers in the list. After a call is redirected four times (makes four hops), it is redirected to the final number.

```
ephone-hunt 10 peer
 pilot 450
 list 451, 452, 453, 477
 final 500
 max-timeout 10
 timeout 3, 3, 3, 3
```

Example for Longest-idle Ephone-Hunt Group

The following example defines longest-idle ephone hunt group 1 with a pilot number 7501 and 11 numbers in the list. After a call is redirected five times, it is redirected to the final number.

```
ephone-hunt 1 longest-idle
 pilot 7501

 list 7001, 7002, 7023, 7028, 7045, 7062, 7067, 7072, 7079, 7085, 7099
 final 8000

 preference 1

 hops 5
 timeout 20

 no-reg
```

Example for Longest-idle Ephone-Hunt Group Using From-Ring Option

The following example defines longest-idle ephone hunt group 1 with a pilot number 7501, a final number 8000, and 11 numbers in the list. Because the **from-ring** command is used, on-hook time stamps will be recorded when calls ring extensions and when calls are answered. After a call is redirected six times (makes six hops), it is redirected to the final number, 8000. The **max-redirect** command is used to increase the number of redirects that are allowed because the number of hops (six) is larger than the default number of redirects that are allowed in the system (five).

```
ephone-hunt 1 longest-idle
 pilot 7501

 list 7001, 7002, 7023, 7028, 7045, 7062, 7067, 7072, 7079, 7085, 7099
 final 8000

 from-ring
 preference 1

 hops 6
 timeout 20


telephony-service
 max-redirect 8
```

Example for Sequential Hunt Group

In the following parallel hunt-group example, when callers dial extension 1000, extension 1001, 1002, 1003, and 1004 ring simultaneously. The first extension to answer is connected. If none of the extensions answers within 60 seconds, the call is forwarded to extension 2000, which is the number for voice mail.

```
voice hunt-group 4 parallel
 final 2000
 list 1001,1002,1003,1004
 timeout 60
 pilot 1000
 preference 1 secondary 9
!
!
ephone-dn  1  octo-line
 number 1001
!
ephone-dn  2
 number 1002
!
ephone-dn  3  dual-line
 number 1003
!
ephone-dn  4
 number 1004
!
!
ephone  1
 max-calls-per-button 4
 mac-address 02EA.EAEA.0001
 button  1:1
!
!
ephone  2
 mac-address 001C.821C.ED23
 button  1:2
!
!
ephone  3
 mac-address 002D.264E.54FA
 button  1:3
!
!
ephone  4
 mac-address 0030.94C3.053E
 button  1:4
```

Example for Preventing Local Call Forwarding in Parallel Voice Hunt-Groups

The following example shows how to prevent the forwarding of local calls to the final destination in parallel voice hunt-group 1:

```
Router# configure terminal
Router(config)# voice hunt-group 1 parallel
Router(config-voice-hunt-group)# no forward local-calls to-final
```

Example for Associating a Name with a Called Voice Hunt-Group

When incoming call A reaches voice hunt group B and lands on final C, extension C does not show the name of the forwarder because the voice hunt group is not configured to display the name. To display the name of the forwarder and the final number, two separate names are required for the primary and secondary pilot numbers.

ephone-hunt

The following is a sample output of the **show run** command when the primary and secondary pilot names are configured in ephone-hunt configuration mode:

```
ephone-hunt 10 sequential
 pilot 1010 secondary 1020
 list 2004, 2005
 final 2006
 timeout 8, 8
 name "EHUNT PRIMARY" secondary "EHUNT SECONDARY"

ephone-hunt 11 peer
 pilot 1012 secondary 1022
 list 2004, 2005
 final 2006
 timeout 8, 8
 name EHUNT1 secondary EHUNT1-SEC
```

The following is a sample output of the **show ephone-hunt** command when the primary and secondary pilot names are configured in ephone-hunt configuration mode:

```
show ephone-hunt 10
Group 10
type: sequential
pilot number: 1010, peer-tag 20010
pilot name: EHUNT PRIMARY
secondary number: 1020, peer-tag 20011
secondary name: EHUNT SECONDARY
```

voice hunt-group

The following example shows how the primary and secondary pilot names are configured in voice hunt-group configuration mode:

```
voice hunt-group 24 parallel
final 097
list 885,886,124,154
timeout 20
pilot 021 secondary 621
name SALES secondary SALES-SECONDARY
```

The following is a sample output of the **show voice hunt-group** command when the primary and secondary pilot names are configured in voice hunt-group configuration mode:

```
show voice hunt-group 1
Group 1
type: parallel
pilot number: 1000, peer-tag 2147483647
secondary number: 2000, peer-tag 2147483646
```

pilot name: SALES
secondary name: SALES-SECONDARY
```
list of numbers:
  Member Used-by State  Login/Logout
  ====== ======  =====  ==========
  2004   2004    up     login
  2005   2005    down   -
preference: 0
preference (sec): 0
timeout: 180
final_number:
stat collect: no
phone-display: no
```

Example for Specifying a Description for a Voice Hunt-Group

The following example shows how to specify a description for voice hunt-group 12 using the **description** command and presents the description in the output of the **do show run** command:

```
Router(config)# voice hunt-group 12 parallel
Router (config-voice-hunt-group)# description ?
 LINE  description for this hunt group
Router (config-voice-hunt-group)# description specific huntgroup description


Router (config-voice-hunt-group)# do show run | sec voice hunt-group
voice hunt-group 12 parallel
 timeout 0
description specific huntgroup description
```

Example for Logout Display

In the following example, the description is set to "Marketing Hunt Group." This information will be shown in the configuration output and also on the display of IP phones that are receiving calls from this hunt group. The display-logout message is set to "Night Service," which will be displayed on IP phones that are members of the hunt group when all the members are logged out.

```
ephone-hunt 17 sequential
 pilot 3000
 list 3011, 3021, 3031
 timeout 10
 final 7600
 description Marketing Hunt Group
 display-logout Night Service
```

Example for Displaying Total Logged-In Time and Total Logged-Out Time for Each Hunt-Group Agent

The following example displays the duration (in sec) since a specific agent logged into and logged out of ephone hunt group 1 from 4:00 a.m. to 5:00 a.m. (0400 to 0500):

show ephone-hunt 1 statistics
```
Wed 04:00 - 05:00
 Max Agents: 3
 Min Agents: 3
 Total Calls: 9
 Answered Calls: 7
 Abandoned Calls: 2
 Average Time to Answer (secs): 6
```

```
Longest Time to Answer (secs): 13
Average Time in Call (secs): 75
Longest Time in Call (secs): 161
Average Time before Abandon (secs): 8
Calls on Hold: 2
Average Time in Hold (secs): 16
Longest Time in Hold (secs): 21
Per agent statistics:
 Agent: 5012
  From Direct Call:
   Total Calls Answered: 3
   Average Time in Call (secs): 70
   Longest Time in Call (secs): 150
   Totals Calls on Hold: 1
   Average Hold Time (secs): 21
   Longest Hold Time (secs): 21
  From Queue:
   Total Calls Answered: 3
   Average Time in Call (secs): 55
   Longest Time in Call (secs): 78
   Total Calls on Hold: 2
   Average Hold Time (secs): 19
   Hold Time (secs): 26
  Total logged in Time (secs) : 3000
  Total logged out Time (secs) : 600

 Agent: 5013
  From Direct Call:
   Calls Answered: 3
   Average Time in Call (secs): 51
   Longest Time in Call (secs): 118
   Totals Calls on Hold: 1
   Average Hold Time (secs): 11
   Longest Hold Time (secs): 11
  From Queue:
   Total Calls Answered: 1
   Average Time in Call (secs): 4
   Longest Time in Call (secs): 4
  Total logged in Time (secs) : 3000
  Total logged out Time (secs) : 600

 Agent: 5014
  From Direct Call:
   Total Calls Answered: 1
   Average Time in Call (secs): 161
   Longest Time in Call (secs): 161
  From Queue:
   Total Calls Answered: 1
   Time in Call (secs): 658
   Longest Time in Call (secs): 658
  Total logged in Time (secs) : 3000
  Total logged out Time (secs) : 600

Queue related statistics:
 Total calls presented to the queue: 5
 Calls handoff to IOS: 5
 Number of calls in the queue: 0
 Average time to handoff (secs): 2
 Longest time to handoff (secs): 3
 Number of abandoned calls: 0
 Average time before abandon (secs): 0
 Calls forwarded to voice mail: 0
 Calls answered by voice mail: 0
 Number of error calls: 0
```

Note The per agent statistics are displayed for both static and dynamic agents.

Example for Dynamic Membership To Ephone-Hunt

The following example creates four ephone-dns and a hunt group that includes the first ephone-dn and two wildcard slots. The last three ephone-dns are enabled for group hunt dynamic membership. Each of them can join and leave the hunt group whenever one of the wildcard slots is available. Standard FACs have been enabled, and the agents use standard FACs to join (*3) and leave (#3) the hunt group. You can also use the **fac** command to create custom FACs for these actions if you prefer.

```
ephone-dn 22
 number 4566

ephone-dn 24
 number 4568
 ephone-hunt login

ephone-dn 25
 number 4569
 ephone-hunt login

ephone-dn 26
 number 4570
 ephone-hunt login

ephone-hunt 1 peer
 list 4566,*,*
 timeout 10
 final 7777

telephony-service
 fac standard
```

Example for Dynamic Membership To Voice Hunt-Group

The following example creates one voice register dn and one voice hunt group which includes two wildcard slots. The voice register dn is enabled for group hunt dynamic membership. The DN can join and unjoin the hunt group whenever one of the wildcard slots is available. Standard FACs have been enabled, and the agents use standard FACs to join (*3) and unjoin (#3) the hunt group. You can also use the **fac** command to create custom FACs for these actions if you prefer.

```
Voice register dn 1
Number 1001
Voice-hunt-groups login

Voice hunt-group 1 parallel
Pilot number 100
List 1001, 1002, 1003, *, *
```

Example for Agent Status Control using SCCP Phones

The following example sets up a peer ephone hunt group. It also establishes the appearance and order of soft keys for phones that are configured with ephone-template 7. These phones will have the HLog key available when they are idle, when they have seized a line, or when they are connected to a call. Phones without softkeys can use the standard HLog codes to toggle ready and not-ready status.

```
ephone-hunt 10 peer
 pilot 450
 list 451, 452, 453, 477
 final 500
 timeout 45
telephony-service
 hunt-group logout HLog
 fac standard
ephone-template 7
 softkeys connected Endcall Hold Transfer HLog
 softkeys idle Newcall Redial Pickup Cfwdall HLog
 softkeys seized Endcall Redial Pickup Cfwdall HLog
```

Example for Agent Status Control using SIP Phones

The following example sets up a peer voice hunt group. It also establishes the appearance and order of soft keys for phones that are configured with voice register template 7. These phones will have the HLog key available when idle, when there is a ringIn, or when connected to a call. Phones without softkeys can use the standard HLog codes to toggle ready and not-ready status.

```
voice hunt-group 10 peer
 pilot 450
 list 451, 452, 453, 477
 final 500
 timeout 45

telephony-service
 hunt-group logout HLog
 fac standard

voice register template 7
 softkeys connected Endcall Hold Transfer HLog
 softkeys idle Newcall Redial Pickup Cfwdall HLog
 softkeys ringIn Answer DND iDivert HLog
```

Example for Automatic Agent Not-Ready for Ephone Hunt Group

The following example enables automatic status change to not-ready after one unanswered hunt group call (the default) for both dynamic and static hunt group members (the default). It also specifies that the phones which are automatically put into the not-ready status should only be blocked from further hunt-group calls and that they should be able to receive calls that directly dial their extensions.

```
ephone-hunt 3 peer
 pilot 4200
 list 1001, 1002, 1003
 timeout 10
 auto logout
 final 4500
telephony-service
 hunt-group logout HLog
```

The following example enables automatic status change to not-ready after two unanswered hunt group calls for any ephone-dn that dynamically logs in to the hunt group using the wildcard slot in the hunt group list.

Phones that are automatically placed in the not-ready status when they do not answer two hunt-group calls are also placed into DND status (they will also not accept directly dialed calls).

```
ephone-hunt 3 peer
 pilot 4200
 list 1001, 1002, *
 timeout 10
 auto logout 2 dynamic
 final 4500
telephony-service
 hunt-group logout DND
```

Example for Automatic Agent Not-Ready for Voice Hunt Group

In the following example, voice hunt-group 1 is configured to permit automatic logout. If hunt group calls that are presented to 1001, 1002, 1003, and 1004 are unanswered (that is, if they ring longer than 40 seconds each), voice register pool 1, voice register pool 2, ephone 1, and ephone 2 are automatically logged out. All unanswered calls are sent to DN 5000.

```
Router(config)# voice register dn 1
Router(config-register-dn)# number 1001
Router(config)# voice register dn 2
Router(config-register-dn)# number 1002

Router(config)# ephone-dn 1
Router(config-ephone-dn)# number 1003
Router(config)# ephone-dn 2
Router(config-ephone-dn)# number 1004

Router(config)# voice register pool 1
Router(config-register-pool)# number 1 dn 1

Router(config)# voice reister pool 2
Router(config-register-pool)# number 1 dn 2

Router(config)# ephone 1
Router(config-ephone)# button 1:1

Router(config)# ephone 2
Router(config-ephone)# button 1:2

Router(config)# voice hunt-group 1 peer
Router(config-voice-hunt)# pilot 1111
Router(config-voice-hunt)# list 1001, 1002, 1003, 1004
Router(config-voice-hunt)# final 5000
Router(config-voice-hunt)# timeout 40
Router(config-voice-hunt)# auto logout 4
```

Example for Call Statistics From a Voice Hunt Group

The following is a sample output from the **show voice hunt-group statistics** command. The output includes direct calls to a voice hunt group number and calls from queue/B-ACD.

```
Router# show voice hunt-group 1 statistics last 1 h
Wed 04:00 - 05:00
 Max Agents: 3
 Min Agents: 3
 Total Calls: 9
 Answered Calls: 7
 Abandoned Calls: 2
 Average Time to Answer (secs): 6
 Longest Time to Answer (secs): 13
```

```
Average Time in Call (secs): 75
Longest Time in Call (secs): 161
Average Time before Abandon (secs): 8
Calls on Hold: 2
Average Time in Hold (secs): 16
Longest Time in Hold (secs): 21
Per agent statistics:
 Agent: 5012
  From Direct Call:
   Total Calls Answered: 3
   Average Time in Call (secs): 70
   Longest Time in Call (secs): 150
   Totals Calls on Hold: 1
   Average Hold Time (secs): 21
   Longest Hold Time (secs): 21
  From Queue:
   Total Calls Answered: 3
   Average Time in Call (secs): 55
   Longest Time in Call (secs): 78
   Total Calls on Hold: 2
   Average Hold Time (secs): 19
   Longest Hold Time (secs): 26
   Total Loged in Time (secs): 3000
   Total Loged out Time (secs): 600
 Agent: 5013
  From Direct Call:
   Total Calls Answered: 3
   Average Time in Call (secs): 51
   Longest Time in Call (secs): 118
   Totals Calls on Hold: 1
   Average Hold Time (secs): 11
   Longest Hold Time (secs): 11
  From Queue:
   Total Calls Answered: 1
   Average Time in Call (secs): 4
   Longest Time in Call (secs): 4
   Total Loged in Time (secs): 3000
   Total Loged out Time (secs): 600
 Agent: 5014
  From Direct Call:
   Total Calls Answered: 1
   Average Time in Call (secs): 161
   Longest Time in Call (secs): 161
  From Queue:
   Total Calls Answered: 1
   Average Time in Call (secs): 658
   Longest Time in Call (secs): 658
   Total Loged in Time (secs): 3000
   Total Loged out Time (secs): 600

Queue related statistics:
 Total calls presented to the queue: 5
 Calls handoff to IOS: 5
 Number of calls in the queue: 0
 Average time to handoff (secs): 2
 Longest time to handoff (secs): 3
 Number of abandoned calls: 0
 Average time before abandon (secs): 0
 Calls forwarded to voice mail: 0
 Calls answered by voice mail: 0
 Number of error calls: 0
```

Note The per agent statistics are displayed for both static and dynamic agents.

Example for Night Service on SCCP Phones

The following example provides night service before 8 a.m. and after 5 p.m. Monday through Friday, before 8 a.m. and after 1 p.m. on Saturday, and all day Sunday. Extension 1000 is designated as a night-service extension. Incoming calls to extension 1000 during the night-service period ring on extension 1000 and provide night-service notification to phones that are designated as night-service phones. In this example, the night-service phones are ephone 14 and ephone 15. The night-service notification consists of a single ring on the phone and a display of "Night Service 1000." A night-service toggle code has been configured, *6483 (*NITE), by which a phone user can activate or deactivate night-service conditions during the hours of night service.

```
telephony-service
 night-service day mon 17:00 08:00
 night-service day tue 17:00 08:00
 night-service day wed 17:00 08:00
 night-service day thu 17:00 08:00
 night-service day fri 17:00 08:00
 night-service day sat 13:00 12:00
 night-service day sun 12:00 08:00
 night-service code *6483
!
ephone-dn 1
 number 1000
 night-service bell
!
ephone-dn 2
 number 1001
 night-service bell
!
ephone-dn 10
 number 2222
!
ephone-dn 11
 number 3333
!
ephone 5
 mac-address 1111.2222.0001
 button 1:1 2:2
!
ephone 14
 mac-address 1111.2222.0002
 button 1:10
 night-service bell
!
ephone 15
 mac-address 1111.2222.0003
 button 1:11
 night-service bell
```

Example for Night Service on SIP Phones

The following example provides night service everyday before 10:00 am and after 7:00 pm. Incoming calls to extension 3000 during the night-service period ring on extension 3000 and provide night-service notification to phones that are designated as night-service phones. In this example, the night-service phones are pool 2 and pool 3. The night-service notification consists of a single ring on the phone and a display of "Night Service 3000." A night-service toggle code has been configured, *8765 (*NITE), by which a phone user can activate or deactivate night-service conditions during the hours of night service.

```
telephony-service
night-service everyday 19:00 10:00
night-service code *8765

voice register dn 1
```

```
number 3000
night-service bell

voice register dn 2
number 3001
night-service bell

voice register dn 10
number 5555

voice register dn 11
number 6666

voice register pool 1
mac-address 1111.2222.0001
number 1 dn 1
number 2 dn 2

voice register pool 2
mac-address 1111.2222.0002
number 1 dn 10
night-service bell

voice register pool 3
mac-address 1111.2222.0003
number 1 dn 11
night-service bell
```

Examples for Overlaid Ephone-dns

Example for Overlaid Ephone-dn

The following example creates three lines (ephone-dns) that are shared across three IP phones to handle three simultaneous calls to the same telephone number. Three instances of a shared line with the extension number 1001 are overlaid onto a single button on each of three phones. A typical call flow is as follows. The first call goes to ephone 1 (highest preference) and rings button 1 on all three phones (huntstop is off). The call is answered on ephone 1. A second call to extension 1001 hunts onto ephone-dn 2 and rings on the two remaining ephones, 11 and 12. The second call is answered by ephone 12. A third simultaneous call to extension 1001 hunts onto ephone-dn 3 and rings on ephone 11, where it is answered. Note that the no huntstop command is used to allow hunting for the first two ephone-dns, and the huntstop command is used on the final ephone-dn to stop call-hunting behavior. The preference command is used to create different selection preferences for each ephone-dn.

```
ephone-dn 1
 number 1001
 no huntstop
 preference 0

ephone-dn 2
 number 1001
 no huntstop
 preference 1

ephone-dn 3
 number 1001
 huntstop
 preference 2

ephone 10
 button 1o1,2,3
 ephone 11
 button 1o1,2,3

ephone 12
 button 1o1,2,3
```

Example for Overlaid Dual-Line Ephone-dn

The following example shows how to overlay dual-line ephone-dns. In addition to using the **huntstop** and **preference** commands, you must use the **huntstop channel** command to prevent calls from hunting to the second channel of an ephone-dn. This example overlays five ephone-dns on button 1 on five different ephones. This allows five separate calls to the same number to be connected simultaneously, while occupying only one button on each phone.

```
ephone-dn 10 dual-line
 number 1001
 no huntstop
 huntstop channel
 preference 0

ephone-dn 11 dual-line
 number 1001
 no huntstop
 huntstop channel
 preference 1

ephone-dn 12 dual-line
 number 1001
 no huntstop
 huntstop channel
 preference 2

ephone-dn 13 dual-line
 number 1001
 preference 3
 no huntstop
 huntstop channel

ephone-dn 14 dual-line
 number 1001
 preference 4
 huntstop
 huntstop channel

ephone 33
 mac 00e4.5377.2a33
 button 1o10,11,12,13,14

ephone 34
 mac 9c33.0033.4d34
 button 1o10,11,12,13,14

ephone 35
 mac 1100.8c11.3865
 button 1o10,11,12,13,14

ephone 36
 mac 0111.9c87.3586
 button 1o10,11,12,13,14

ephone 37
 mac 01a4.8222.3911
 button 1o10,11,12,13,14
```

Example for Shared-line Overlaid Ephone-dns

The following is an example of a unique ephone-dn as the primary dn in a simple shared-line overlay configuration. The **no huntstop** command is configured for all the ephone-dns except ephone-dn 12, the last one in the overlay set. Because the ephone-dns are dual-line dns, the **huntstop-channel** command is also configured to ensure that the second channel remains free for outgoing calls and for conferencing.

```
ephone-dn 1 dual-line
 number 101
 huntstop-channel
!
ephone-dn 2 dual-line
 number 102
 huntstop-channel
!
ephone-dn 10 dual-line
 number 201
 no huntstop
 huntstop-channel
!
ephone-dn 11 dual-line
 number 201
 no huntstop
 huntstop-channel
!
ephone-dn 12 dual-line
 number 201
 huntstop-channel
!
!The following ephone configuration includes (unique) ephone-dn 1 as the primary line in a
 shared-line overlay
ephone 1
 mac-address 1111.1111.1111
 button 1o1,10,11,12
!
!The next ephone configuration includes (unique) ephone-dn 2 as the primary line in another
 shared-line overlay
!
ephone 2
 mac-address 2222.2222.2222
 button 1o2,10,11,12
```

Example for Overlaid Ephone-dn with Call Waiting

In following example, button 1 on ephone 1 though ephone 3 uses the same set of overlaid ephone-dns with call waiting that share the number 1111. The button also accept calls to each ephone's unique (nonshared) ephone-dn number. Note that if ephone-dn 10 and ephone-dn 11 are busy, the call will go to ephone-dn 12. If ephone-dn 12 is busy, the call will go to voice mail.

```
ephone-dn 1 dual-line
 number 1001

ephone-dn 2 dual-line
 number 1001

ephone-dn 3 dual-line
 number 1001

ephone-dn 10 dual-line
 number 1111
 no huntstop
 huntstop channel
 call-forward noan 7000 timeout 30

ephone-dn 11 dual-line
 number 1111
 preference 1
 no huntstop
 huntstop channel
 call-forward noan 7000 timeout 30

ephone-dn 12 dual-line
 number 1111
 preference 2
 huntstop channel
 call-forward noan 7000 timeout 30
 call-forward busy 7000

ephone 1
 button 1c1,10,11,12

ephone 2
 button 1c2,10,11,12

ephone 3
 button 1c3,10,11,12
```

Example for Overlaid Ephone-dns with Rollover Buttons

The following example configures a “3x3” shared-line setup for three ephones and nine shared lines (ephone-dns 20 to 28). Each ephone has a unique ephone-dn for each of its three buttons (ephone-dns 11 to 13 on ephone 1, ephone-dns 14 to 16 on ephone 2, and ephone-dns 17 to 19 on ephone 3). The rest of the ephone-dns are shared among the three phones. Three phones with three buttons each can take nine calls. The overflow buttons provide the ability for an incoming call to ring on the first available button on each phone.

```
ephone-dn 11
 number 2011

ephone-dn 12
 number 2012

ephone-dn 13
 number 2013

ephone-dn 14
 number 2014
.
.
.
ephone-dn 28
 number 2028

ephone 1
 button 1o11,12,13,20,21,22,23,24,25,26,27,28 2x1 3x1

ephone 2
 button 1o14,15,16,20,21,22,23,24,25,26,27,28 2x1 3x1

ephone 3
 button 1o17,18,19,20,21,22,23,24,25,26,27,28 2x1 3x1
```

Example for Called-Name Display for Voice Hunt Group

The Called-Name Display feature supports the display of the name associated with a called number for incoming calls to IP phones configured on Unified CME. For an example of Called-Name Display for Voice Hunt Group calls, see Example for Called-Name Display for Voice Hunt Group, on page 672.

Example for Called Directory Name Display for Overlaid Ephone-dns

The following example demonstrates the display of a directory name for a called ephone-dn that is part of an overlaid ephone-dn set. For configuration information, see Directory Services, on page 659.

This configuration of overlaid ephone-dns uses wildcards in the secondary numbers for the ephone-dns. Wildcards allow you to control the display according to the number that was dialed. The example is for a medical answering service with three IP phones that accept calls for nine doctors on one button. When a call to 5550101 rings on button 1 on phone 1 to phone 3, “doctor1” is displayed on all three phones.

```
telephony-service
```

```
 service dnis dir-lookup
 directory entry 1 5550101 name doctor1
 directory entry 2 5550102 name doctor2
 directory entry 3 5550103 name doctor3
 directory entry 4 5550110 name doctor4
 directory entry 5 5550111 name doctor5
 directory entry 6 5550112 name doctor6
 directory entry 7 5550120 name doctor7
 directory entry 8 5550121 name doctor8
 directory entry 9 5550122 name doctor9
ephone-dn 1
 number 5500 secondary 555000.
ephone-dn 2
 number 5501 secondary 555001.
ephone-dn 3
 number 5502 secondary 555002.
ephone 1
 button 1o1,2,3
 mac-address 1111.1111.1111
ephone 2
 button 1o1,2,3
 mac-address 2222.2222.2222
ephone 3
 button 1o1,2,3
 mac-address 3333.3333.3333
```

The following example shows a hunt-group configuration for a medical answering service with two phones and four doctors. Each phone has two buttons, and each button is assigned two doctors' numbers. When a patient calls 5550341, Cisco Unified CME matches the hunt-group pilot secondary number (555....), rings button 1 on one of the two phones, and displays "doctor1." For more information about hunt-group behavior, see Hunt Groups, on page 1248. Note that wildcards are used only in secondary numbers and cannot be used with primary numbers.

```
telephony-service

 service dnis dir-lookup
 max-redirect 20
 directory entry 1 5550341 name doctor1
 directory entry 2 5550772 name doctor1
 directory entry 3 5550263 name doctor3
 directory entry 4 5550150 name doctor4
ephone-dn 1
 number 1001
ephone-dn 2
 number 1002
ephone-dn 3
 number 1003
ephone-dn 4
 number 104
ephone 1
 button 1o1,2
 button 2o3,4
 mac-address 1111.1111.1111
ephone 2
 button 1o1,2
 button 2o3,4
 mac-address 2222.2222.2222
ephone-hunt 1 peer
 pilot 5100 secondary 555....
 list 1001, 1002, 1003, 1004
 final number 5556000
 hops 5
 preference 1

 timeout 20

 no-reg
```

Example for Called Ephone-dn Name Display for Overlaid Ephone-dns

The following example demonstrates the display of the name assigned to the called ephone-dn using the **name** command. For information about configuring this feature, see Directory Services, on page 659.

In this example, three phones have button 1 assigned to pick up three shared 800 numbers for three different catalogs.

The default display for the phones is the number of the first ephone-dn listed in the overlay set (18005550100). A call is made to the first ephone-dn (18005550100), and the caller ID (for example, 4085550123) is visible on all phones. The user for phone 1 answers the call. The caller ID (4085550123) remains visible on phone 1, and the displays on phone 2 and phone 3 return to the default display (18005550100). A call to the second ephone-dn (18005550101) is made. The default display on phone 2 and phone 3 is replaced with the called ephone-dn's name (catalog1) and number (18005550101).

```
telephony-service
 service dnis overlay
ephone-dn 1
 number 18005550100
ephone-dn 2
 name catalog1
 number 18005550101
ephone-dn 3
 name catalog2
 number 18005550102
ephone-dn 4
 name catalog3
 number 18005550103
ephone 1
 button 1o1,2,3,4
ephone 2
 button 1o1,2,3,4
ephone 3
 button 1o1,2,3,4
```

Example for OOD-R

```
voice register global
mode cme
source-address 11.1.1.2 port 5060
load 7971 SIP70.8-0-1-11S
load 7970 SIP70.8-0-1-11S
load 7961GE SIP41.8-0-1-0DEV
load 7961 SIP41.8-0-1-0DEV
authenticate ood-refer
authenticate credential 1 tftp://172.18.207.15/labtest/cred1.csv
create profile sync 0004550081249644
...
sip-ua
authentication username
```

Where to Go Next

Dial-Peer Call Hunt and Hunt Groups

Dial peers other than ephone-dn dial peers can be directly configured as hunt groups or rotary groups, in which multiple dial peers can match incoming calls. (These are not the same as Cisco Unified CME ephone hunt groups.) For more information, see the “Hunt Groups” section of the Dial Peers Features and Configuration chapter of Dial Peer Configuration on Voice Gateway Routers.

Called-Name Display

This feature allows you to specify that the name of the called party, rather than the number, should be displayed for incoming calls. This feature is very helpful for agents answering calls for multiple ephone-dns that appear on a single line button in an ephone-dn overlay set. For more information, see Directory Services, on page 659.

Soft Key Control

If the **hunt-group logout** command is used with the **HLog** keyword, the HLog soft key appears on phones during the idle, connected, and seized call states. The HLog soft key is used to toggle an agent from the ready to not-ready status or from the not-ready to ready status. To move or remove the HLog soft key on one or more phones, create and apply an ephone template that contains the appropriate **softkeys** commands.

From Unified CME Release 11.6 onwards, HLog keyword is supported with the **hunt-group logout** command configured under telephony service. On SIP phone, HLog softkey appears on phone for idle, ringIn, and connected state.

For more information, see Customize Softkeys, on page 925.

Feature Access Codes (FACs)

Dynamic membership allows agents at authorized ephones to join or leave a hunt group using a feature access code (FAC) after standard or custom FACs are enabled.

In Cisco Unified CME 4.0 and later versions, you can activate call pickup using a feature access code (FAC) instead of a soft key when standard or custom FACs have been enabled for your system. The following are the standard FACs for call pickup:

- Pickup group—Dial the FAC and a pickup group number to pick up a ringing call in a different pickup group than yours. Standard FAC is **4.
- Pickup local—Dial the FAC to pick up a ringing call in your pickup group. Standard FAC is **3.
- Pickup direct—Dial the FAC and the extension number to pick up a ringing call at any extension. Standard FAC is **5.

For more information about FACs, see Feature Access Codes, on page 757.

Controlling Use of the Pickup Soft Keys

To block the functioning of the group pickup (GPickUp) or local pickup (Pickup) soft key without removing the key display, create and apply an ephone template that contains the **features blocked** command. For more information, see Configure Call Blocking, on page 1064.

To remove the group pickup (GPickUp) or local pickup (Pickup) soft key from one or more phones, create and apply an ephone template that contains the appropriate **softkeys** command. For more information, see Customize Softkeys, on page 925.

Ephone-dn Templates

The **ephone-hunt login** command authorizes an ephone-dn to dynamically join and leave an ephone hunt group. It can be included in an ephone-dn template that is applied to one or more individual ephone-dns. For more information, see Templates, on page 1427.

Ephone Hunt Group Statistics Reports

Several different types of statistics can help you track whether your current ephone hunt groups are meeting your call coverage needs. These statistics can be displayed on-screen or written to files.

For more information, see the Cisco Unified CME Basic Automatic Call Distribution and Auto-Attendant Service chapter in Cisco Unified CME B-ACD and Tcl Call-Handling Applications.

Voice Hunt Group Statistics Reports

The **hunt-group statistics write-all** command writes all the ephone and voice hunt group statistics to a file.

The **hunt-group statistics write-v2** command writes all the ephone and voice hunt group statistics to a file, along with total logged in and logged out time for agents.

The **statistics collect** command enables the collection of call statistics for a voice hunt group.

The **show telephony-service all** command displays the total number of ephone and voice hunt groups that have statistics collection turned on.

The **show voice hunt-group statistics** command displays call statistics from voice hunt groups.

For more information, see Cisco Unified Communications Manager Express Command Reference.

Do Not Disturb

The Do Not Disturb (DND) feature can be used as an alternative to the HLog function for preventing incoming calls from ringing on a phone. The difference is that HLog prevents only hunt group calls from ringing, while DND prevents all calls from ringing. For more information, see Do Not Disturb, on page 679.

Automatic Call Forwarding During Night-Service

To have an ephone-dn forward all its calls automatically during night-service hours, use the **call-forward night-service** command. For more information, see Enable Call Forwarding for a Directory Number, on page 1185.

Ephone Templates

The **night-service bell** command specifies that a phone will receive night-service notification when calls are received at ephone-dns configured as night-service ephone-dns. This command can be included in an ephone template that is applied to one or more individual ephones.

For more information, see Templates, on page 1427.

Feature Information for Call Coverage Features

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

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

Table 106: Feature Information for Call Coverage

Feature Name	Cisco Unified CME version	Modification
Call Hunt	3.4	Added support for configuring call hunt features on SIP IP phones connected directly to Cisco Unified CME.
	3.0	• Preference for secondary numbers was introduced. • Huntstop was introduced.
	1.0	• Ephone-dn dial-peer preference was introduced. • Huntstop was introduced.
Call Pickup	7.1	Added Call Pickup support for SIP phones.
	4.0	• The ability to globally disable directed call pickup was introduced. • Feature access codes for call pickup were introduced. • The ability to block call pickup on individual phones was introduced.
	3.2	The ability to remove or rearrange soft keys on individual phones was introduced.
	3.0	Call pickup groups were introduced.
Call Waiting	8.0	Added Cancel Call Waiting feature.
	3.4	Added support for configuring call waiting for SIP phones directly connected to Cisco Unified CME.
Callback Busy Subscriber	3.0	Callback busy subscriber was introduced.

Feature Name	Cisco Unified CME version	Modification
Hunt Groups		
	7.0/4.3	Added support for the following: • SCCP phones in Voice Hunt-Groups • Call Forwarding to a Parallel Voice Hunt-Group (Blast Hunt Group) • Call Transfer to a Voice Hunt-Group • Member of Voice Hunt-Group can be a SCCP phone, FXS analog phone, DS0-group, PRI-group, SIP phone, or SIP trunk

Feature Name	Cisco Unified CME version	Modification
Hunt Groups	4.0	

Feature Name	Cisco Unified CME version	Modification
		Added support for the following on IP phones running SCCP: • Maximum number of hunt groups in a system was increased from 20 to 100 and maximum number of agents in a hunt group was increased from 10 to 20. • Maximum number of hops automatically adjusts to the number of agents. • A description can be added to phone displays and configuration output to provide hunt group information associated with ringing and answered calls. • A configurable message can be displayed on agent phones when all agents are in the not-ready status to advise the destination to which calls are being forwarded or other useful information. • No-answer timeouts can be set individually for each ephone-dn in the list and a cumulative no-answer timeout can be set for all ephone-dns. • Automatic logout trigger criterion was changed from exceeding the specified timeout to exceeding the specified number of calls. The name of this feature was changed from automatic logout to automatic agent status not-ready. • Dynamic hunt group membership is introduced. Agents can join and leave hunt groups whenever a wildcard slot is available. • Agent status control using an

Feature Name	Cisco Unified CME version	Modification
		HLog soft key or feature access code (FAC) is introduced. Agents can put their lines into not-ready state to temporarily block hunt group calls without relinquishing their slots in group. • Calls can be blocked from agent phones that are not idle or on hook. • Calls that are not answered by the hunt group can be returned to the party who transferred them into the huntgroup. • Calls parked by hunt group agents can be returned to a different entry point. • (Sequential hunt groups only) Local calls to a hunt group can be restricted so that they will not be forwarded past the initial agent that is rung. • (Longest-idle hunt groups only) A new command, the **from-ring** command, specifies that on-hook time stamps should be updated when a call rings an agent and when a call is answered by an agent.
	3.4	Added support for configuring hunt groups for SIP phones directly connected to Cisco Unified CME.
	3.2.1	• Maximum number of hunt groups in a system was increased to 20. • Automatic logout capability was introduced.
	3.2	

Feature Name	Cisco Unified CME version	Modification
		Longest-idle hunt groups were introduced.
	3.1	Secondary pilot numbers were introduced.
	3.0	Peer and sequential ephone hunt groups were introduced.
Night Service	11.6	Night service support for mixed deployment of SIP and SCCP phone was introduced.
	11.5	Night service support for SIP phone was introduced.
	4.0	The **night-service everyday**, **night-service weekday**, and **night-service weekend** commands were introduced.
	3.3	The behavior of the night-service code was changed. Previously, using the night-service code at a phone either enabled or disabled night service for the ephone-dns on that phone. Now, using the night-service code at a phone enables or disables night service for all night-service ephone-dns.
	3.0	Night service was introduced.

Feature Name	Cisco Unified CME version	Modification
Overlaid Ephone-dns	4.0	• The number of ephone-dns that can be overlaid on a single button using the **button** command and the o or c keyword was increased from 10 to 25. • The ability to extend calls for overlaid ephone-dns to other buttons (rollover buttons) on the same phone was introduced. Rollover buttons are created by using the x keyword with the **button** command. • The number of waiting calls that can be displayed for overlaid ephone-dns that have call waiting configured has been increased to six for the following phone types: Cisco Unified IP Phone 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G, and 7971G-GE.
	3.2.1	Call waiting for overlaid ephone-dns was introduced and the c keyword was added to the **button** command.
	3.0	Overlaid ephone-dns were introduced and the o keyword was added to the **button** command.
Voice Hunt Group Enhancements	11.6	Hlog Softkey support for SIP Phones was introduced.
	9.0	Allows all ephone and voice hunt group call statistics to be written to a file using the **hunt-group statistics write-all** command.

Feature Name	Cisco Unified CME version	Modification
Preventing Local-Call Forwarding to Final Agent in Voice Hunt Groups	9.5	The **no forward local-calls** command was introduced in ephone-hunt group to prevent a local call from being forwarded to the next agent.
Enhancement of Support for Hunt Group	9.5	Hunt group agent statistics of Cisco Unified SCCP IP phones is enhanced to include Total logged in time and Total logged out.
Total Logged in and Logged out Time Statistics for agent	9.5	Allows all ephone hunt call statistics to be written to a file along with total logged in and logged out time for agents using the **hunt-group statistics write-v2** command.
Enhancement of Support for Total Logged in and Logged out Time Statistics for Agent	11.5	Allows all voice hunt call statistics to be written to a file along with total logged in and logged out time for agents using the **hunt-group statistics write-v2** command.
Out-of-Dialog Refer	4.1	Out-of Dialog REFER support was added.

CHAPTER 45

Caller ID Blocking

Restrictions for Caller ID Blocking

Caller ID blocking on outbound calls does not apply to PSTN calls through foreign exchange office (FXO) ports. Caller ID features on FXO-connected subscriber lines are under the control of the PSTN service provider, who may require you to subscribe to their caller ID blocking service.

Information About Caller ID Blocking

Caller ID Blocking on Outbound Calls

Phone users can block caller-ID displays on calls from a particular ephone-dn, or you can selectively choose to block the name or number on outbound calls from a particular dial peer.

The display of caller ID information for outgoing calls from a particular ephone-dn can be blocked on a per-call basis, allowing users to maintain their privacy when necessary. The system administrator defines a code for caller ID blocking in Cisco Unified CME. Users then dial the code before making any call on which they do not want their number displayed on the called-party phone. The caller ID is sent, but its presentation parameter is set to “restricted” so that the caller ID is not displayed.

Blocking CLID displays for local calls from a particular extension tells the far-end gateway device to block display of calling-party information for the calls received from this ephone-dn.

Alternatively, you can allow the local display of CLID information and independently block the CLID name or number on outbound VoIP calls. This configuration has the benefit of allowing caller-ID display for local calls while preventing caller-ID display for external calls going over VoIP. This feature can be used for PSTN calls that go out over ISDN.

Configure Caller ID Blocking

Block Caller ID For All Outbound Calls on SCCP Phones

To block the CLID name or number on outbound VoIP calls from a particular dial peer, perform the following steps.

Restriction

- Caller ID continues to be displayed for local calls. To block caller ID display on all outbound calls from a particular directory number, use the **caller-id block** command. See Block Caller ID From a Directory Number on SCCP Phones, on page 1365 or Verify Caller ID Blocking, on page 1366.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* [**pots** |**voip**]
4. **clid strip**
5. **clid strip name**
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	**dial-peer voice** *tag* [**pots** |**voip**] **Example:** `Router(config)# dial-peer voice 3 voip`	Enters dial-peer configuration mode. **Note** You can configure caller-ID blocking on POTS dial peers if the POTS interface is ISDN. This feature is not available on FXO/CAS lines.

	Command or Action	Purpose
Step 4	**clid strip** **Example:** `Router(config-dial-peer)# clid strip`	(Optional) Removes the calling-party number from the CLID information being sent with VoIP calls.
Step 5	**clid strip name** **Example:** `Router(config-dial-peer)# clid strip name`	(Optional) Removes the calling-party name from the CLID information being sent with VoIP calls.
Step 6	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Block Caller ID From a Directory Number on SCCP Phones

To define a code that phone users can dial to block caller ID display on selected outbound calls from a particular directory number or to block caller ID display on all calls from a directory number, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **caller-id block code** *code-string*
5. **exit**
6. **ephone-dn** *dn-tag*
7. **caller-id block**
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**caller-id block code** *code-string* **Example:** `Router(config-telephony)# caller-id block code *1234`	(Optional) Defines a code that users can enter before making calls on which the caller ID should not be displayed. • *code-string*—Digit string of up to 16 characters. The first character must be an asterisk (*).
Step 5	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 6	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 3`	Enters ephone-dn configuration mode.
Step 7	**caller-id block** **Example:** `Router(config-ephone-dn)# caller-id block`	(Optional) Blocks display of caller-ID information for all outbound calls that originate from this directory number. This command can also be configured in ephone-dn-template configuration mode and applied to one or more directory number. The ephone-dn configuration has priority over the ephone-dn-template configuration.
Step 8	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Verify Caller ID Blocking

Use the **show running-config** command to display caller ID blocking parameters, which may appear in the telephony-service, ephone-dn, or dial-peer portions of the output.

Example:

```
Router# show running-config

dial-peer voice 450002 voip
 translation-profile outgoing 457-456
 destination-pattern 457
 session target ipv4:10.43.31.81
 dtmf-relay h245-alphanumeric
 codec g711ulaw
 no vad
 clid strip
!
telephony-service
 fxo hook-flash
 load 7960-7940 P00305000600
 load 7914 S00103020002
 max-ephones 100
 max-dn 500
 ip source-address 10.115.34.131 port 2000
 max-redirect 20
 no service directed-pickup
 timeouts ringing 10
 system message XYZ Company
 voicemail 7189
 max-conferences 8 gain -6
 moh music-on-hold.au
 caller-id block code *1234
 web admin system name cisco password cisco
 dn-webedit
 time-webedit
 transfer-system full-consult
 transfer-pattern 92......
 transfer-pattern 91..........
 transfer-pattern 93......
 transfer-pattern 94......
 transfer-pattern 95......
 transfer-pattern 96......
 transfer-pattern 97......
 transfer-pattern 98......
 transfer-pattern .T
 secondary-dialtone 9
 after-hours block pattern 1 91900 7-24
 after-hours block pattern 2 9976 7-24
!
 create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
!
ephone-dn  2  dual-line
 number 126
 preference 1
 call-forward busy 500
 caller-id block
```

Configuration Examples for Caller ID Blocking

Example for Configuring Caller ID Blocking Code

The following example defines a code of *1234 for phone users to enter to block caller ID on their outgoing calls:

```
telephony-service
 caller-id block code *1234
```

Example for Configuring Caller ID Blocking for Outbound Calls from a Directory Number on SCCP Phones

The following example sets CLID blocking for the ephone-dn with tag 3.

```
ephone-dn 3
 number 2345
 caller-id block
```

The following example blocks the display of CLID name and number on VoIP calls but allows CLID display for local calls:

```
ephone-dn 3
 number 2345
dial-peer voice 2 voip
 clid strip
 clid strip name
```

Feature Information for Caller ID Blocking

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

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

Table 107: Feature Information for Caller ID Blocking

Feature Name	Cisco Unified CME Version	Feature Information
Caller ID Blocking	3.0	Caller ID blocking per local call was introduced.
	1.0	Caller ID blocking for outbound calls was introduced.

CHAPTER 46

Conferencing

Restrictions for Conferencing

When you are configuring dial peers or ephone-dns, including park slots and conferencing extensions, on Cisco Integrated Services Router Voice Bundles, the following message may appear to warn you that free memory is not available:

%DIALPEER_DB-3-ADDPEER_MEM_THRESHOLD: Addition of dial-peers limited by available memory

To configure more dial peers or ephone-dns, increase the DRAM in the system. A moderately complex configuration may exceed the default 256 MB DRAM and require 512 MB DRAM. Note that many factors contribute to memory usage, in addition to the number of dial peers and ephone-dns configured.

Information About Conferencing

Conferencing Overview

Conferencing allows you to join three or more parties in a telephone conversation. Two types of conferencing are available in Cisco Unified CME: ad hoc and meet-me.

Ad hoc conferences can be hardware-based or software-based. Software-based conferences use the router CPU to provide audio mixing (G.711) and are limited to 3 parties. Hardware-based multi-party ad hoc conferencing uses digital signal processors (DSPs) to allow more parties than software-based ad hoc conferencing and also provides additional features such as Join and Conference Participant List (ConfList).

Meet-me conferences are created by parties calling a designated conference number. Meet-me conferencing is hardware-based only. If you configure software-based conferencing, you cannot have meet-me conferences.

From Cisco Unified CME Release 11.7, hardware conferencing is supported on Cisco 4000 Series Integrated Services Router.

Conferencing with Octo-Lines

In Cisco Unified CME 4.3 and later versions, when a conference initiator is an octo-line directory number, Cisco Unified CME selects an idle channel from that directory number and the user must establish a new call to complete the conference. If an idle channel is not available on the same octo-line directory number, the conference aborts and a "`No Line Available`" message displays. Cisco Unified CME does not select an idle channel from another directory number and the user cannot select "hold" calls on the other channels of the directory number or other directory numbers, which is the behavior for single-line and dual-line directory numbers.

With octo-line directory numbers, only one directory number is required for an 8-party meet-me or ad hoc conference. Up to eight select and join instances are supported.

Secure Conferencing Limitation

Cisco Unified CME cannot use the secure conference DSP farm capability. If Cisco Unified CME needs a conference DSP farm resource for multiparty ad hoc or meet-me conferencing, it will use a secure or nonsecure DSP farm resource depending on what resources have been registered with Cisco Unified CME. If Cisco Unified CME happens to pick a secure DSP farm resource, the conference itself will not be secure, which is a waste, in terms of sessions capacity, of the more expensive secure DSP farm resource.

To avoid using valuable secure DSP farm resources, we recommend that you do not register a secure conference DSP Farm profile to a Cisco Unified CME because Cisco Unified CME cannot use the DSP farm's secure capabilities.

Ad-hoc Conferencing

Before Cisco Unified CME 4.1, support for conferencing is limited to three-party ad hoc conference calls using a G.711 codec. To have an ad hoc conference with a party that is not using a G.711 codec, transcoding is necessary. For more information, see Transcoding When a Remote Phone Uses G.729r8, on page 478.

From Unified CME 11.7 onwards, conference participants (line or trunk) with different codecs can be added to the conference bridge without the need for configuring extra DSP resources for transcoding. During a two-party transcoded call on Unified CME (Cisco 4000 Series Integrated Services Router), LTI-based transcoding is invoked. When the two-party call becomes an Ad-hoc conference, LTI-based transcoding is released and SCCP-based DSP conference is invoked. The DSP inserted for conferencing would take care of both transcoding and mixing the audio stream.

The maximum number of simultaneous conferences is platform-specific to the type of Cisco Unified CME router, and each individual Cisco Unified IP phone can host a maximum of one conference at a time. You cannot create a second conference on a phone if you already have an existing conference on hold.

Conference Gain Levels

In Cisco Unified CME 3.3 and later versions, you can adjust the gain level of an external call to provide more adequate volume. This functionality is applied to inbound audio packets so that conference participants can more clearly hear a remote PSTN or VoIP caller joining their call. Note that this functionality cannot discriminate between a remote VoIP/foreign exchange office (FXO) source, which requires a volume gain, and a remote VoIP/IP phone, which does not require a volume gain and may therefore incur some sound distortions.

End-of-Conference Options

For Cisco CME 3.2 and later versions, a person who initiates a conference call and hangs up can either keep the remaining parties connected or disconnect them.

Cisco Unified IP phones can be configured to keep the remaining conference parties connected when the conference initiator hangs up (places the handset back in the on-hook position). Conference originators can disconnect from their conference calls by pressing the Confrn (conference) soft key. When an initiator uses the Confrn key to disconnect from the conference call, the oldest call leg will be put on hold, leaving the initiator connected to the most recent call leg. The conference initiator can then navigate between the two parties by pressing either the Hold soft key or the line buttons to select the desired call.

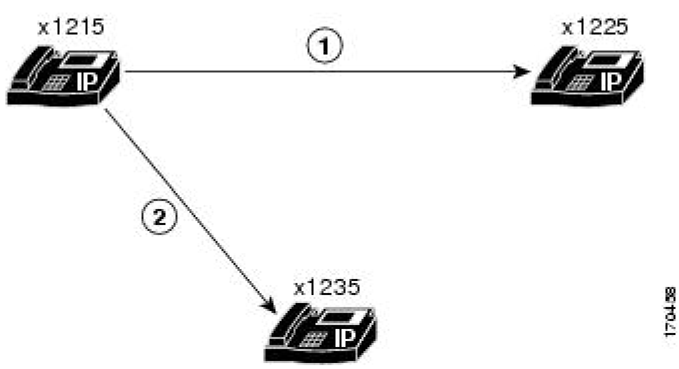
In Cisco Unified CME 4.0 and later versions, behavior for the end of three-way conferences can be configured at a phone level. The options specify whether the last party that joined a conference can be dropped from the conference and whether the remaining two parties should be allowed to continue their connection after the conference initiator has left the conference.

Multi-Party Ad Hoc Conferencing for More Than Three Parties

In Cisco Unified CME 4.1 and later versions, hardware-based multi-party ad hoc conferences allow more than three parties. Ad hoc conferences are created when one party calls another, then either party decides to add another party to the call. Ad hoc conferences can be created in several ways.

The conference shown in Figure 64: Simple AdHoc Conference Using the Conf Soft Key, on page 1371 is created when extension 1215 dials extension 1225. The two parties decide to add a third party, extension 1235. Extensions 1215, 1225, and 1235 are now parties in an ad hoc conference. Extension 1215 is the creator.

Figure 64: Simple AdHoc Conference Using the Conf Soft Key



You can configure ad hoc conferencing so that only the creator can add parties to the conference. The default is that any party can add other parties to the conference. You can configure conferencing so that the conference drops when the creator hangs up, and you can configure it so that the conference drops when the last local party hangs up. The default is that the conference is not dropped, regardless of whether the creator hangs up, provided three parties remain in the conference.

From Cisco Unified CME Release 11.7, when the creator transfers the call or parks the call with another call, the conference bridge remains active. The conference is not dropped, even when the **drop-mode creator** command is enabled.

From Cisco Unified CME Release 11.7, Multi-Party Ad Hoc Conferencing is supported on Cisco 4000 Series Integrated Services Router. The maximum number of conference parties you can support on a conference call is limited to 8. Hardware-based multi-party ad hoc conference bridges does not support video phones. In a scenario where the participants joins the conference with video enabled phones, the caller on that phone can connect to the conference as an audio only participant.

Also, when the participant puts the call on hold in a conference, the other parties in the conference remain connected. The Resume softkey is not displayed to the other active remote-in-use calls on the shared lines. Only, the participant who puts the call on hold can resume the call.

For configuration information, see Configure Conferencing Options on SCCP Phones, on page 1379 section for more information.

Connected Conference

Connected Conference supports a consultation call for conference in connected call state. In a connected call scenario for SIP phones, a line on the phone is in an active call. The other lines are in held state. Using the Connected conference feature, the user can allow one of the calls on hold to join the active call.

Note For Connected Conference to work on phones, Ad Hoc conferencing has to be enabled on Unified CME.

Connected Conference is supported only on Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series.

Only one held call can join the active call at a time for SIP phones. If the other lines on the SIP phone has to join the conference, they can join one at a time. A maximum of 8 participants can be part of a connected conference.

From Cisco Unified CME Release 11.7 onwards, Connected Conference feature is supported on SIP phones as well. As part of this enhancement, a new softkey **Active calls** has been added to the SIP phones configured on Unified CME.

For the Connected Conference feature, the behavior is different across Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series. For Cisco IP Phone 7800 Series, line key is used by the Connected Conference feature. However, **Active calls** softkey is used in Cisco IP Phone 8800 Series.

Following are the steps to invoke connected conferencing on Cisco IP Phone 8800 Series:

1. A call from Phone A (Cisco IP Phone 8800 Series) is answered by Phone B.
2. Phone A puts the call with Phone B on hold.
3. Phone A makes another call to Phone C, and the call is answered by Phone C.
4. Press the **Conference** hard button or softkey on Phone A.
5. Then, press the **Active calls** softkey on Phone A to select the option Phone B.
6. Repeat the above steps to add more parties into conference.

A connected conference between Cisco IP Phone 8800 Series Phone A, Phone B, and Phone C is established.

Following are the steps to invoke connected conferencing on Cisco IP Phone 7800 Series:

1. A call from Phone A (Cisco IP Phone 7800 Series) is answered by Phone B.
2. Phone A puts the call with Phone B on hold.
3. Phone A makes another call to Phone C, and the call is answered by Phone C.
4. Use the line key on Phone A to select the option Phone B.
5. Repeat the above steps to add more parties into conference.

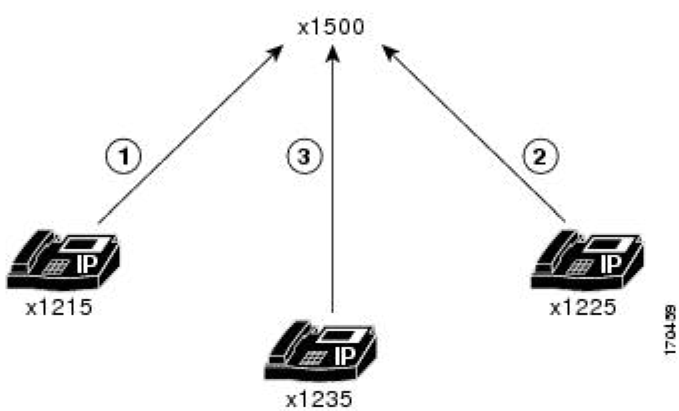
A connected conference between Cisco IP Phone 7800 Series IP Phone A, Phone B, and Phone C is established.

Note The phone firmware files that support Connected Conference on Cisco IP Phone 8800 Series is unavailable until the next Unified CME release. Hence, Connected Conference support for SIP phones is limited to Cisco IP Phone 7800 Series for Unified CME Release 11.7.

Meet-Me Conferencing in Cisco Unified CME 4.1 and Later versions

In Cisco Unified CME 4.1 and later versions, meet-me conferences consist of at least three parties dialing a meet-me conference number predetermined by a system administrator. For example, the conference shown in Figure 65: Simple Meet-Me Conference Scenario, on page 1373 is created when the conference creator at extension 1215 presses the MeetMe soft key and hears a confirmation tone, then dials the meet-me conference number 1500. Extension 1225 and extension 1235 join the meet-me conference by dialing 1500. Extensions 1215, 1225, and 1235 are now parties in a meet-me conference on extension 1500.

Figure 65: Simple Meet-Me Conference Scenario



Configure Maximum Parties

You can configure the maximum number of conference parties to be lower than the actual maximum of 32 for meet-me conferences. See Configure the DSP Farm Profile on SCCP Phones, on page 1387 the section for more information.

Freeing Conference Resources

If only one party remains in the meet-me conference, for example, if one party has forgotten to hang up, the conference call is disconnected after five minutes to free system resources.

If the creator is waiting for parties to join the conference and is the only party on the conference, the conference is not disconnected because significant resources are not being used.

Meet-Me Conferencing in Cisco Unified CME 11.7 and Later Versions

From Cisco Unified CME Release 11.7, Meet-Me conferencing is supported on Cisco 4000 Series Integrated Services Router. The Meet-Me conference requires a minimum of three parties dialing a Meet-Me conference number, predetermined by the system administrator. The maximum number of conference parties you can support on a conference call is limited to 32. However, you can configure the number of participants that can attend a Meet-Me conference.

Configuration of multi-party conference on Cisco 4000 Series ISRs for Unified CME Release 11.7 and later is same as that of previous releases. Also, the configuraton remains same across both SIP and SCCP phones. For more information, see Configure Conferencing, on page 1377

Soft Keys for Conference Functions

In Cisco Unified CME 4.1 and later versions, the following soft keys provide conferencing functions for hard-ware based multi-party conferencing enhancements on your phone and require the appropriate DSP farm configuration. For configuration information, see Configure Multi-Party Ad Hoc and Meet-Me Conferencing in Cisco Unified CME 4.1 and Later Versions on SCCP Phones, on page 1383.

- ConfList—Conference list. Lists all parties in a conference. For multi-party ad hoc conferences, this soft key is available for all parties in a conference. For meet-me conferences, this soft key is available for the creator only. Press **Update** to update the list of parties in the conference, for instance, to verify that a party has been removed from the conference. Press **Remove** softkey to remove the appropriate parties. The suboption **Remove** is available for the conference creator and phones that have **conference admin** configured.
- Join—Joins an established call to an adhoc conference. You must first press **Select** to choose each connected call that you want to join in a conference, then press **Join** to join the selected calls to the conference.
- RmLstC—Remove last caller. Removes the last party added to the conference. This soft key works for the creator only.
- Select—Selects a call or conference to join to a conference and selects a call to remove from a conference. The creator can remove other parties by pressing the **ConfList** soft key, then use the **Select** and **Remove** soft keys to remove the appropriate parties.
- MeetMe—Initiates a meet-me conference. The creator presses this soft key before dialing the conference number. Other meet-me conference parties only dial the conference number to join the conference. This soft key must be configured before you can initiate meet-me conferences.

In Cisco Unified CME 11.7 and later versions, the following softkeys are also supported.

- Details (Supported only on Cisco IP Phone 7800 Series)—Lists all the participants in a conference. For multi-party ad hoc conferences, this soft key is available for all parties in a conference. For meet-me conferences, this soft key is available for the creator only. Press **Update** to update the list of parties in the conference. Press **Remove** softkey to remove the appropriate parties. The suboption **Remove** is available to the conference creator and phones that have **conference admin** configured.

- Show detail (Supported only on Cisco IP Phone 8800 Series)—Lists all the participants in a conference. For multi-party ad hoc conferences, this soft key is available for all parties in a conference. For meet-me conferences, this soft key is available for the creator only. Press **Update** to update the list of parties in the conference. Press **Remove** softkey to remove the appropriate parties. The suboption **Remove** is available to the conference creator and phones that have **conference admin** configured.

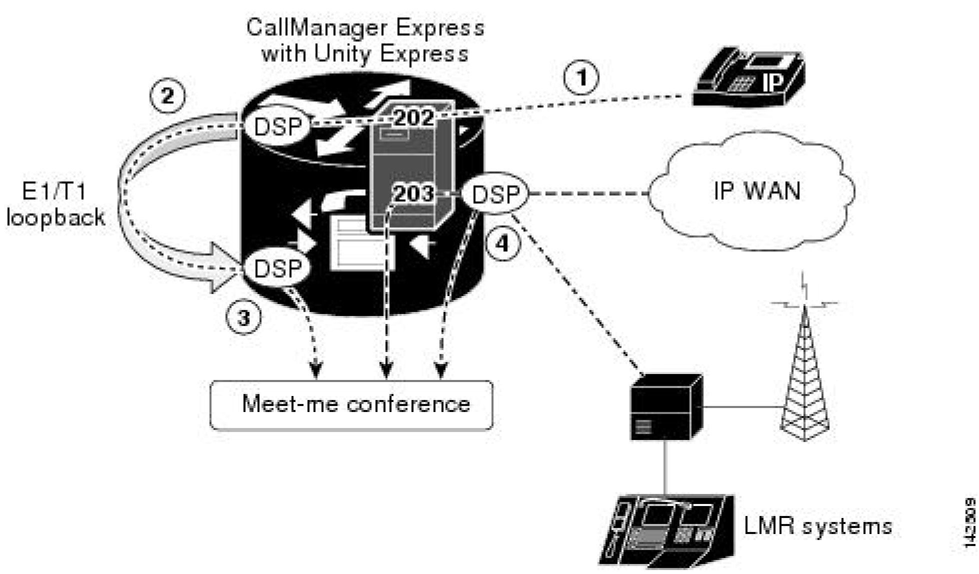
Meet-Me Conferencing in Cisco CME 3.2 to Cisco Unified CME 4.0

Unlike the built-in Cisco Unified CME conference feature, a meet-me conference does not have a three-party limit. Meet-me Conferencing in Cisco CME 3.2 to Cisco Unified CME 4.0 requires Cisco Unity Express auto-attendant to transfer callers to the correct Meet-Me bridge and a dual T-1/E-1 VWIC card for providing DSP resources. By default three Meet-Me bridge's with 8 callers each are defined with the maximum number of callers restricted by the number of DSP resources available in the Cisco router. A maximum of 96 callers in conference is supported. Multicast conferences can be accessed from IP phones, public switched telephone network (PSTN) callers, and Cisco Land Mobile Radio (LMR) devices connected to ear and mouth (E&M) voice ports on the Cisco Unified CME router.

The only limiting factor for this solution is the number of T1 or E1 loopback ports and digital-signal-processor (DSP) resources available.

Figure 66: Meet-Me Conference in Cisco CME 3.2 to Cisco Unified CME 4.0, on page 1375 illustrates the callflow for Meet-Me Conferencing on a Cisco router with Cisco CME 3.2 to Cisco Unified CME 4.0 and Cisco Unity Express. IP phones and PSTN callers dial into Cisco Unity Express Auto Attendant using separate access numbers. Cisco Unity Express Auto Attendant routes calls to a multicast conference based on which access number is called. In this example, local IP phones call 202 and PSTN users call 203 to dial into Cisco Unity Express.

Figure 66: Meet-Me Conference in Cisco CME 3.2 to Cisco Unified CME 4.0



1 In order to send or receive audio from a multicast conference, calls must pass through a DSP for audio mixing. By default, IP phone calls are not passed through a DSP. IP phone calls can be routed to T1 or

E1 loopback, forcing the call to pass through a DSP. In this example, Cisco Unity Express routes callers who dialed 202, through the E1/T1 loopback.

2. The T1/E1 loopback ports are permanently trunked to the multicast conference. Incoming calls to T1 loopback are routed back to the multicast conference on Cisco CME.
3. All PSTN calls must pass through a DSP, so incoming PSTN calls do not have to be routed to T1 loopback. The Auto Attendant routes PSTN calls directly to the multicast conference. In this example, Cisco Unity Express routes callers who dialed 203 directly into the multicast conference.
4. Cisco LMR ports are permanently trunked into the multicast conference, so radio parties can listen to audio from both the IP phone and the PSTN. Pushing the "talk" button on a radio handset keys the M lead on the Cisco CME E&M port and the radio handset can transmit audio.

Note Cisco LMR devices typically cannot transmit and receive audio at the same time. If a Cisco LMR device receives audio from a multicast conference, it cannot transmit audio. In order for a Cisco LMR device to transmit audio to the conference, all IP phone and PSTN parties must be on mute so the LMR device does not receive any audio. If a single IP phone or PSTN device in the conference is transmitting audio, the individual using the Cisco LMR device cannot talk.

Dial Plan

Before configuring Cisco Unified CME and Cisco Unity Express, you should plan your dial plan for Meet-Me Conferencing. Table 108: Dial Plan for Support Meet-Me Conferencing, on page 1376 lists the dial-plan parameters that must be defined before you can configure Meet-Me Conferencing in Cisco CME 3.2 to Cisco Unified CME 4.0.

To prevent IP phones from dialing into the multicast bridge directly, the multicast bridge numbers should be set to nondialable numbers starting with an alphabetical character.

IP phones that dial into the multicast bridge cannot send or receive audio, so IP phone calls must be routed to the loopback number. These numbers are required to configure Cisco Unity Express Auto Attendant, which controls all access to the multicast bridge.

Table 108: Dial Plan for Support Meet-Me Conferencing

Parameter	Sample Number	Description
External Number	203	Number used by external callers from PSTN to dial into Cisco Unity Express Auto Attendant conference bridge.
Internal Number	202	Number used by internal callers from local IP phones to dial into Cisco Unity Express Auto Attendant conference bridge.

Parameter	Sample Number	Description
bridge1	212	Number used by Cisco Unified CME to route calls to E1 or T1 loopback that is trunked to multicast bridge 1.
bridge2	213	Number used by Cisco Unified CME to route calls to E1 or T1 loopback that is trunked to multicast bridge 2
bridge3	214	Number used by Cisco Unified CME to route calls to E1 or T1 loopback that is trunked to multicast bridge 3.
bridge1_pstn	A212	Nondialable number used by Cisco Unified CME to route calls into multicast bridge 1. Number should start with an alphabetical number.
bridge2_pstn	A213	Nondialable number used by Cisco Unified CME to route calls into multicast bridge 2. Number should start with an alphabetical number.
bridge3_pstn	A214	Nondialable number used by Cisco Unified CME to route calls into multicast bridge 3. Number should start with an alphabetical number.
operator	150	Number dialed if user needs assistance.

Configure Conferencing

Modify the Default Configuration for Three-Party Ad Hoc Conferencing

To globally modify the default configuration and change any of the following parameters for three-party ad hoc conferencing, perform the following steps.

- Maximum number of three-party conferences that are supported simultaneously by the Cisco Unified CME router. Maximum number of simultaneous three-party conferences supported by a router is platform-dependent. The default value is half of the maximum number.
- Increase the sound volume of VoIP and public switched telephony network (PSTN) parties joining a conference call.

Restriction

- When a three-way conference is established, a participant cannot use call transfer to join the remaining conference participants to a different number.
- Three-party ad hoc conferencing does not support meet-me conferences.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **max-conferences** *max-conference-number* [**gain -6** | **0** | **3** | **6**]
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	**telephony-service** **Example:** `Router(config)#`	Enters telephony-service configuration mode.
Step 4	**max-conferences** *max-conference-number* [**gain -6** | **0** | **3** | **6**] **Example:** `Router(config-telephony)# max-conferences 6`	Sets the maximum number of simultaneous three-party conferences supported by the router. • *max-conference-number*—Maximum value is platform-dependent. Type **?** for maximum value. Default is half of the maximum value. • **gain**—(Optional) Amount to increase the sound volume of VoIP and PSTN calls joining a conference call, in decibels. Valid values are **-6**, **0**, **3**, and **6**. The default is **-6**.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

Configure Conferencing Options on SCCP Phones

To configure optional end-of-conference options for three-party ad hoc conferencing on a Cisco Unified IP phone running Skinny Client Control Protocol (SCCP), perform the following steps for each phone to be configured.

Before You Begin

- Conferencing uses call transfer to connect the two remaining parties of a conference when a conference initiator leaves the conference. To use this feature, you must configure the **transfer-system** command. For configuration information, see Configure Call Transfer and Forwarding, on page 1178.
- Drop-last feature of Keep Conference on analog phones connected to the Cisco Unified CME system through a Cisco VG 224 requires Cisco IOS Release 12.4(9)T or later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **keep-conference** [**drop-last**] [**endcall**] [**local-only**]
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** *phone-tag*	Enters ephone configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# ephone 1`	• *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 4	**keep-conference** [**drop-last**] [**endcall**] [**local-only**] **Example:** `Router(config-ephone)# keep-conference endcall`	Allows conference initiators to exit from conference calls and to either end or maintain the conference for the remaining parties. • **no keep-conference**—(Default; the **no** form of the command) The conference initiator can hang up or press the EndCall soft key to end the conference and disconnect all parties or press the Confrn soft key to drop only the last party that was connected to the conference. • **keep-conference**—(No keywords used) The conference initiator can press the EndCall soft key to end the conference and disconnect all parties or hang up to leave the conference and keep the other two parties connected. The conference initiator can also use the Confrn soft key (IP phone) or hookflash (analog phone) to break up the conference but stay connected to both parties. • **drop-last**—The action of the Confrn soft key is changed; the conference initiator can press the Confrn soft key (IP phone) or hookflash (analog phone) to drop the last party. • **endcall**—The action of the EndCall soft key is changed; the conference initiator can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected. • **local-only**—The conference initiator can hang up to end the conference and leave the other two parties connected only if one of the remaining parties is local to the Cisco Unified CME system (an internal extension).
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

What to Do Next

If you are finished modifying the configuration, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Profiles for SIP Phones, on page 391.

Configure Conferencing Options on SIP Phones

To configure optional end-of-conference options for three-party ad hoc conferencing on a Cisco Unified IP phone running SIP, perform the following steps for each phone to be configured.

Restriction Music on hold (MOH) is not supported for call hold invoked from a SIP phone. A caller hears only silence when placed on hold by a SIP phone.

Before You Begin

- To facilitate call transfer by using the Confrn soft key, conference, and transfer attended or transfer blind must be enabled. For configuration information, see Configure Call Transfer and Forwarding, on page 1178.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag* | OR **voice register template** *template-tag*
4. **keep-conference**
5. **voice register pool** *pool-tag*
6. **template** *template-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	**voice register pool** *pool-tag* | OR **voice register template** *template-tag* **Example:** `Router(config)#` **voice register pool 3** OR `Router(config)#` **voice register template 3**	Enters voice register pool or voice register template configuration mode to set phone-specific parameters for SIP phones. • *pool-tag*—Unique sequence number of the SIP phone to be configured. Range is 1 to 100 or the upper limit as defined by **max-pool** command. • *template-tag*—Unique sequence number of the template to be applied to the SIP phone. Range is 1 to 10.
Step 4	**keep-conference** **Example:** `Router(config-register-pool)#` **keep-conference**	Allows a Cisco Unified IP phone conference initiator to exit from conference calls and keeps the remaining parties connected. **Note** This step is included to illustrate how to enable the command if it was previously disabled.

	Command or Action	Purpose
	OR Router(config-register-temp)# **keep-conference**	• Default is enabled. • Remaining calls are transferred without consultation as enabled by the **transfer-attended** (voice register template) or **transfer-blind** (voice register template) commands. **Note** **keep-conference** command is configured under voice register template only if you configure voice register template command in the previous step.
Step 5	**voice register pool** *pool-tag* **Example:** Router(config-register-temp)# **voice register pool 1**	(Optional) Enters voice register pool configuration mode to set phone-specific parameters for SIP phones. **Note** This step is required only if you configure voice register template.
Step 6	**template** *template-tag* **Example:** Router(config-register-pool)# **template 1**	(Optional) Attaches the template tag configured to the voice register pool. **Note** This step is required only if you configure voice register template.
Step 7	**end** **Example:** Router(config-register-pool)# **end**	Exits to privileged EXEC mode.

What to Do Next

- If you are finished modifying the configuration, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Profiles for SIP Phones, on page 391.

Verify Three-Party Ad Hoc Conferencing

Use the **show running-config** command to verify your configuration. Any non-default conferencing parameters are listed in the telephony-service portion of the output, and end-of-conference options are listed in the ephone portion.

Example:

```
Router# show running-config
!
ephone-dn  1  dual-line
 ring feature secondary
 number 126 secondary 1261
 description Sales
```

```
 name Smith
 call-forward busy 500 secondary
 call-forward noan 500 timeout 10
 huntstop channel
 no huntstop
 no forward local-calls
!
ephone  1
 mac-address 011F.92A0.C10B
 type 7960 addon 1 7914
 no dnd feature-ring
 keep-conference
```

Troubleshooting Three-Party Ad Hoc Conferencing

Use the **debug ephone** commands to observe messages and states associated with an ephone. For more information, see Cisco Unified CME Command Reference.

Configure Multi-Party Ad Hoc and Meet-Me Conferencing in Cisco Unified CME 4.1 and Later Versions on SCCP Phones

Prerequisites

- Cisco Unified CME 4.1 or a later version
- You must have a PVDM2-8, PVDM2-16, PVDM2-32, or PVDM2-64 high-density packet voice digital signal processor module hosted on the motherboard or on a module such as the NM-HDV2 or NM-HD-2VE.
- For Cisco Unified IP Phone 7985, firmware version 4-1-2-0 or a later version

Restriction

- The maximum number of meet-me conference parties is 32 for one DSP using the G.711 codec and 16 for the G.729 codec.
- A participant cannot join more than one conference at the same time.
- Hardware-based multi-party ad hoc conferencing for more than three parties is not supported on phones that do not support soft keys.
- Hardware-based multi-party ad hoc conferencing does not support the local-consult transfer method (**transfer-system local-consult** command).

Enable DSP Farm Services for a Voice Card

To enable DSP farm services for a voice card to support multi-party ad hoc and meet-me conferences, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dsp services dspfarm**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice-card** *slot* **Example:** `Router(config)# voice-card 2`	Enters voice-card configuration mode and configure a voice card.
Step 4	**dsp services dspfarm** **Example:** `Router(config-voicecard)# dsp services dspfarm`	Enables digital-signal-processor (DSP) farm services for a particular voice network module.
Step 5	**exit** **Example:** `Router(config-voicecard)# exit`	Exits voice-card configuration mode.

Configure Join and Leave Tones on SCCP Phones

To configure tones to be played when parties join and leave multi-party ad hoc conferences and meet-me conferences, perform the following steps for each tone to be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class custom-cptone** *cptone-name*
4. **dualtone conference**
5. **frequency** *frequency-1*[*frequency-2*]
6. **cadence** {*cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time*] [*cycle-3-on-time cycle-3-off-time*] [*cycle-4-on-time cycle-4-off-time*] |**continuous**}
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 class custom-cptone** *cptone-name* **Example:** `Router(config)# voice class custom-cptone jointone`	Creates a voice class for defining custom call-progress tones to be detected.
Step 4	**dualtone conference** **Example:** `Router(cfg-cptone)# dualtone conference`	Configures conference join and leave tones.
Step 5	**frequency** *frequency-1*[*frequency-2*] **Example:** `Router(cfg-cp-dualtone)# frequency 600 900`	Defines the frequency components for a call-progress tone.
Step 6	**cadence** {*cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time*] [*cycle-3-on-time cycle-3-off-time*] [*cycle-4-on-time cycle-4-off-time*] |**continuous**} **Example:** `Router(cfg-cp-dualtone)# cadence 300 150 300 100 300 50`	Defines the tone-on and tone-off durations for a call-progress tone.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(cfg-cp-dualtone)# exit`	Exits configuration mode and enters privileged EXEC mode.

Configure SCCP for Cisco Unified CME

To enable SCCP on Cisco Unified CME to support multi-party ad hoc and meet-me conferences, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-typeinterface-number* [**port** *port-number*]
4. **sccp ccm** {**ip-address** | *dns*} **identifier** *identifier-number* [**port** *port-number*][**version** *version-number*]
5. **sccp ccm group** *group-number*
6. **bind interface** *interface-type interface-number*
7. **exit**
8. **sccp**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sccp local** *interface-typeinterface-number* [**port** *port-number*] **Example:** `Router(config)# sccp local FastEthernet0/0`	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco Unified CME.

	Command or Action	Purpose
Step 4	**sccp ccm** {**ip-address** | *dns*} **identifier** *identifier-number* [**port** *port-number*][**version** *version-number*] **Example:** `Router(config)# sccp ccm 10.4.158.3 identifier 100 version 4.0`	Enables the Cisco Unified CME router to register SCCP applications. • *version-number*—Must be set to **4.0** or later.
Step 5	**sccp ccm group** *group-number* **Example:** `Router(config)# sccp ccm group 123`	Creates a Cisco Unified CME group.
Step 6	**bind interface** *interface-type interface-number* **Example:** `Router(config-sccp-cm)# bind interface fastethernet 0/0`	Binds an interface to a Cisco Unified CME group.
Step 7	**exit** **Example:** `Router(config-sccp-cm)# exit`	Exits SCCP Cisco Unified CME configuration mode.
Step 8	**sccp** **Example:** `Router(config)# sccp`	Enables SCCP and its related applications (transcoding and conferencing).
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configure the DSP Farm Profile on SCCP Phones

To configure the DSP farm profile for multi-party ad hoc and meet-me conferencing, perform the following steps.

Note The DSP farm can be on the same router as the Cisco Unified CME or on a different router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dspfarm profile** *profile-identifier* **conference**
4. **codec** {*codec-type* | **pass-through**}
5. **conference-join custom-cptone** *cptone-name*
6. **conference-leave custom-cptone***cptone-name*
7. **maximum conference-participants** *max-participants*
8. **maximum sessions** *number*
9. **associate application sccp**
10. **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	**dspfarm profile** *profile-identifier* **conference** **Example:** `Router(config)# dspfarm profile 1 conference`	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
Step 4	**codec** {*codec-type* | **pass-through**} **Example:** `Router(config-dspfarm-profile)# codec g711ulaw`	Specifies the codecs supported by a DSP farm profile. **Note** Repeat this step as necessary to specify all the supported codecs.
Step 5	**conference-join custom-cptone** *cptone-name* **Example:** `Router(config-dspfarm-profile)# conference-join custom-cptone jointone`	Associates a custom call-progress tone to indicate joining a conference with a DSP farm profile. **Note** The *cptone-name* argument in this step must be the same as the *cptone-argument* in the **voice class custom-cptone** command configured in Enable DSP Farm Services for a Voice Card, on page 1384.

	Command or Action	Purpose
Step 6	**conference-leave custom-cptone***cptone-name* **Example:** `Router(config-dspfarm-profile)# conference-leave custom-cptone leavetone`	Associates a custom call-progress tone to indicate leaving a conference with a DSP farm profile. **Note** The *cptone-name* argument in this step must be the same as the *cptone-argument* in the **voice class custom-cptone** command configured in Enable DSP Farm Services for a Voice Card, on page 1384.
Step 7	**maximum conference-participants** *max-participants* **Example:** `Router(config-dspfarm-profile)# maximum conference-participants 32`	(Optional) Configures the maximum number of conference parties allowed in each meet-me conference. The maximum is codec-dependent.
Step 8	**maximum sessions** *number* **Example:** `Router(config-dspfarm-profile)# maximum sessions 8`	Specifies the maximum number of sessions that are supported by the profile.
Step 9	**associate application sccp** **Example:** `Router(config-dspfarm-profile)# associate application sccp`	Associates SCCP with the DSP farm profile.
Step 10	**end** **Example:** `Router(config-dspfarm-profile)# end`	Exits to privileged EXEC mode.

Associate Cisco Unified CME with a DSP Farm Profile on SCCP Phones

To associate a DSP farm profile with a group of Cisco Unified CME routers that control DSP services, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp ccm group** *group-number*
4. **associate ccm** *identifier-number* **priority** *priority-number*
5. **associate profile** *profile-identifier* **register** *device-name*
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	**sccp ccm group** *group-number* **Example:** `Router(config)# sccp ccm group 1`	Creates a Cisco Unified CME group.
Step 4	**associate ccm** *identifier-number* **priority** *priority-number* **Example:** `Router(config-sccp-ccm)# associate ccm 100 priority 1`	Associates a Cisco Unified CME router with the group and establishes its priority within the group.
Step 5	**associate profile** *profile-identifier* **register** *device-name* **Example:** `Router(config-sccp-ccm)# associate profile 2 register confdsp1`	Associates a DSP farm profile with the Cisco Unified CME group. • *device-name* is a maximum of 16 characters. **Note** Repeat this step for every conferencing DSP farm and transcoding DSP farm.
Step 6	**end** **Example:** `Router(config-sccp-ccm)# end`	Exits to privileged EXEC mode.

Enable Multi-Party Ad Hoc and Meet-Me Conferencing

To allow hardware-based multi-party ad hoc conferences with more than three parties and meet-me conferences, perform the following steps.

Note Configuring multi-party ad hoc conferencing in Cisco Unified CME disables three-party (software-based) ad hoc conferencing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **conference hardware**
5. **transfer-system full-consult**
6. **sdspfarm units** *number*
7. **sdspfarm tag** *number device-name*
8. **sdspfarm conference mute-on** *mute-on-digits* **mute-off** *mute-off-digits*
9. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**conference hardware** **Example:** `Router(config-telephony)# conference hardware`	Configures a Cisco Unified CME system for multi-party conferencing only.
Step 5	**transfer-system full-consult** **Example:** `Router(config-telephony)# transfer-system full-consult`	Transfers calls using H.450.2 with consultation using a second phone line, if available. • The calls fall back to full-blind if a second line is not available. • This is the default transfer method in Cisco Unified CME 4.0 and later versions.
Step 6	**sdspfarm units** *number* **Example:** `Router(config-telephony)# sdspfarm units 3`	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.

	Command or Action	Purpose
Step 7	**sdspfarm tag** *number device-name* **Example:** `Router(config-telephony)# sdspfarm tag 2 confdsp1`	Permits a DSP farm to register to Cisco Unified CME and associates it with a SCCP client interface's MAC address. **Note** The *device-name* in this step must be the same as the *device-name* in the **associate profile** command in Step 5 of the section Associate Cisco Unified CME with a DSP Farm Profile on SCCP Phones, on page 1389.
Step 8	**sdspfarm conference mute-on** *mute-on-digits* **mute-off** *mute-off-digits* **Example:** `Router(config-telephony)# sdspfarm conference mute-on 111 mute-off 222`	Defines mute-on and mute-off digits for conferencing. • Maximum: 3 digits. Valid values are the numbers and symbols that appear on your telephone keypad: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, *, and #. • Mute-on and mute-off digits can be the same.
Step 9	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

Configure Multi-Party Ad Hoc Conferencing and Meet-Me Numbers on SCCP Phones

To configure extension numbers for hardware-based multi-party ad hoc and meet-me ad hoc conferencing, based on the maximum number of conference participants you configure, perform the following steps. Ad hoc conferences require four extensions per conference, regardless of how many extensions are actually used by the conference parties.

Note Ensure that you configure enough directory numbers to accommodate the anticipated number of conferences. The maximum number of parties in a multi-party ad hoc conference on an IP phone is eight; the maximum on an analog phone is three.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* **dual-line**
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. Enter one of the following commands:
    - **conference ad-hoc**
    - **conference meetme**
6. **preference** *preference-order* [**secondary** *secondary-order*]
7. **no huntstop**[**channel**]
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	**ephone-dn** *dn-tag* **dual-line** **Example:** `Router(config)# ephone-dn 18 dual-line`	Enters ephone-dn configuration mode to configure an extension (ephone-dn) for a phone line. • Each ephone-dn can carry two parties if it is configured as a dual line. • Configure enough ephone-dns to accommodate the maximum number of conference participants to be supported. • For multi-party ad hoc conferencing, maximum number of directory numbers is 8, but you can configure a lower maximum. • For meet-me conferencing, maximum number of directory numbers is 32, but you can configure a lower maximum. • Minimum number of directory numbers required: 2.
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]	Associates a telephone or extension number with an ephone-dn in a Cisco Unified CME system.

	Command or Action	Purpose
	Example: `Router(config-ephone-dn)# number 6789`	• Each DN for a conference must have the same primary and secondary number.

Step 5	Enter one of the following commands:
	• **conference ad-hoc**
	• **conference meetme**
	
	Example:
	`Router(config-ephone-dn)# conference ad-hoc`
	or
	`Router(config-ephone-dn)# conference meetme`
		Configures a number as a placeholder for ad hoc conferencing to associate the call with the DSP farm.
		or
		(Optional) Associates meet-me conferencing with a directory number.

Step 6	**preference** *preference-order* [**secondary** *secondary-order*] **Example:** `Router(config-ephone-dn)# preference 1`	Sets dial-peer preference order for an extension (ephone-dn) associated with a Cisco Unified IP phone. • Remember to configure “preference x” with low value to last DN. • The lower the value of the *preference-order* argument, the higher the preference of the extension.
Step 7	**no huntstop**[**channel**] **Example:** `Router(config-ephone-dn)# no huntstop`	Continues call hunting behavior for an extension (ephone-dn) or an extension channel. • Remember to configure **no huntstop** for all DNs except the last one.
Step 8	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged EXEC mode.

Configure Conferencing Options for SCCP Phones

To configure a template of conferencing features such as the add party mode, drop party mode, and soft keys for hardware-based multi-party ad hoc and meet-me conferences and apply the template to a phone, perform the following steps.

Note The following commands can also be configured in ephone configuration mode. Commands configured in ephone configuration mode have priority over commands in ephone-template configuration mode.

Restriction

- The ConfList (including the Remove, Update, and Exit soft keys within the ConfList function) and RmLstC soft keys do not work on a Cisco Unified IP Phone 7902, 7935, and 7936.
- The RmLstC, ConfList, Join, and Select functions and soft keys are not supported for software-based conferencing.

Before You Begin

- The RmLstC, ConfList, Join, and Select functions and soft keys are supported for hardware-based conferencing only and require the appropriate DSP farm configuration. For configuration information, see these tasks in this module:
  - Enable DSP Farm Services for a Voice Card, on page 1384
  - Configure the DSP Farm Profile on SCCP Phones, on page 1387
  - Associate Cisco Unified CME with a DSP Farm Profile on SCCP Phones, on page 1389

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **conference add-mode**[**creator**]
5. **conference drop-mode** [| **creator local**]
6. **conference admin**
7. **softkeys connected**{[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]}
8. **softkeys hold** {[**Join**] [**Newcall**] [**Resume**] [**Select**]}
9. **softkeys idle** {[**Cfwdall**] [**ConfList**] [**Dnd**] [**Gpickup**] [**HLog**] [**Join**] [**Login**] [**Newcall**] [**Pickup**] [**Redial**] [**RmLstC**]}
10. **softkeys seized** {[**CallBack**] [**Cfwdall**] [**Endcall**] [**Gpickup**] [**HLog**] [**MeetMe**] [**Pickup**] [**Redial**]}
11. **exit**
12. **ephone** *phone-tag*
13. **ephone-template** *template-tag*
14. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone-template** *template-tag* **Example:** `Router(config)# ephone-template 1`	Enter ephone-template configuration mode to create an ephone template to configure a set of phone features.
Step 4	**conference add-mode**[**creator**] **Example:** `Router(config-ephone-template)# conference add-mode creator`	(Optional) Configures the mode for adding parties to conferences. • **creator—**Only the creator can add parties to the conference.
Step 5	**conference drop-mode** [| **creator local**] **Example:** `Router(config-ephone-template)# conference drop-mode creator`	(Optional) Configures the mode for dropping parties from multi-party ad hoc conferences. • **creator—**The active conference terminates when the creator hangs up. • **local—**The active conference terminates when the last local party in the conference hangs up or drops out of the conference.
Step 6	**conference admin** **Example:** `Router(config-ephone-template)# conference admin`	(Optional) Configures the ephone as the conference administrator. The administrator can: • Dial in to any conference directly through the conference number • Use the ConfList soft key to list conference parties • Remove any party from any conference
Step 7	**softkeys connected**{[**Acct**] [**ConfList**] [**Confrn**] [**Endcall**] [**Flash**] [**HLog**] [**Hold**] [**Join**] [**LiveRcd**] [**Park**] [**RmLstC**] [**Select**] [**TrnsfVM**] [**Trnsfer**]} **Example:** `Router(config-ephone-template)# softkeys connected Hold Trnsfer Park Endcall Confrn ConfList Join Select RmLstC`	Configures an ephone template for softkey display during the connected call stage. • The soft keys used for multi-party conferencing are **RmLstC**,**ConfList**,**Join** , and **Select**. These soft keys are supported for hard-ware based conferencing only and require the appropriate DSP farm configuration. • The number and order of soft key keywords you enter in this command correspond to the number and order of soft keys on your phone.
Step 8	**softkeys hold** {[**Join**] [**Newcall**] [**Resume**] [**Select**]}	Configures an ephone template to modify softkey display during the call-hold call stage.

	Command or Action	Purpose
	Example: `Router(config-ephone-template)# softkeys hold Join Newcall Resume Select`	• The soft keys used for multi-party conferencing are **Join** and**Select**. These soft keys are supported for hard-ware based conferencing only and require the appropriate DSP farm configuration. • The number and order of softkey keywords you enter in this command correspond to the number and order of soft keys on your phone.
Step 9	**softkeys idle** {[**Cfwdall**] [**ConfList**] [**Dnd**] [**Gpickup**] [**HLog**] [**Join**] [**Login**] [**Newcall**] [**Pickup**] [**Redial**] [**RmLstC**]} **Example:** `Router(config-ephone-template)# softkeys idle ConfList Gpickup Join Login Newcall Pickup Redial RmLstC`	Configures an ephone template for softkey display during the idle call stage. • The soft keys used for multi-party conferencing are **RmLstC**,**ConfList**, and **Join**. These soft keys are supported for hard-ware based conferencing only and require the appropriate DSP farm configuration. • The number and order of soft key keywords you enter in this command correspond to the number and order of soft keys on your phone.
Step 10	**softkeys seized** {[**CallBack**] [**Cfwdall**] [**Endcall**] [**Gpickup**] [**HLog**] [**MeetMe**] [**Pickup**] [**Redial**]} **Example:** `Router(config-ephone-template)# softkeys seized Redial Endcall Cfwdall Pickup Gpickup Callback Meetme`	(Optional) Configures an ephone template for softkey display during the seized call stage. • You must configure the **MeetMe** soft key in the seized state for the ephone to initiate a meet-me conference. • The number and order of soft key keywords you enter in this command correspond to the number and order of soft keys on your phone.
Step 11	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 12	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode to create and configure an ephone.
Step 13	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-dn-template 1`	Applies an ephone-dn template to an ephone-dn. **Note** The *template-tag* must be the same as the *template-tag* in Step 3.
Step 14	**end** **Example:** `Router(config-ephone)# exit`	Exits to privileged EXEC mode.

What to Do Next

If you are finished modifying the configuration, you are ready to generate configuration files for the phones to be connected. See Generate Configuration Files for SCCP Phones, on page 388.

Verify Multi-Party Ad Hoc and Meet-Me Conferencing on SCCP Phones

Use the following **show** commands to verify multi-party ad hoc and meet-me conferencing:

- **show ephone-dn conference**—Displays information about ad hoc and meet-me conferences.
- **show telephony-service conference hardware**—Displays information about hardware-based conferences.

Sample Output for **show ephone-dn conference** command

```
    type   active inactive  numbers
=======================================
Meetme     0       8      2345
DN tags: 9, 10, 11, 12

Ad-hoc     0       8      A001
DN tags: 13, 14, 15, 16

Meetme     0       8      1234
DN tags: 20, 21, 22, 23
```

Sample Output for **show telephony-service conference hardware detail command**

```
    Conference   Type    Active  Max  Peak    Master MasterPhone     Last
                                          cur(initial)
==================================================================
8889        Ad-hoc  3     8   3   8044    29    ( 29) 8012
Conference parties:
    8012
    8006
    8044
```

Configure Meet-Me Conferencing in Cisco CME 3.2 to Cisco Unified CME 4.0 on SCCP Phones

See Examples, on page 1400 to configure Meet-Me Conferencing on a Cisco router with Cisco CME 3.2 or a later version and Cisco Unity Express.

Note To configure Meet-Me Conferencing in Cisco Unified CME 4.1 or a later version, see Configure Multi-Party Ad Hoc Conferencing and Meet-Me Numbers on SCCP Phones, on page 1392.

Prerequisites

- Cisco CME 3.2 to Cisco Unified CME 4.0.

- A dual VWIC-2MFT-T1 or E-1 loopback for internal callers. The number of VWIC-2MFT-T1 cards required depends on the number of local IP phones parties that need to dial into the meet-me conference. Each VWIC-2MFT-T1 card can support 24 local IP phone parties.
- Packet Voice DSP Modules (PVDM DSPs) to handle the number of callers in conference. A maximum of 96 conference parties is supported using an approved platform, such as a Cisco 3800 router, with at least two PVDM2-64DSPs installed.
- Your IP network is operational and you can access Cisco web.
- You have a valid Cisco.com account.
- The recommended Cisco IOS release and Cisco Unified CME phone firmware and GUI files to support Cisco Unity Express are installed on the Cisco Unified CME router.
- To determine whether the Cisco IOS software release and Cisco Unified CME software version are compatible with the Cisco Unity Express version, Cisco router model, and Cisco Unity Express hardware that you are using, see Cisco Unity Express Compatibility Matrix.
- To verify installed Cisco Unity Express software version, enter the Cisco Unity Express command environment and use the **show software version** user EXEC command. For information about the command environment, see the appropriate Cisco Unity Express CLI Administrator Guide.
- The proper Cisco Unity Express license for Cisco Unified CME, not Cisco Unified Communications Manager, is installed. To verify installed license, enter the Cisco Unity Express command environment and use the **show software license** user EXEC command. For information about the command environment, see the appropriate Cisco Unity Express CLI Administrator Guide.

This is an example of the Cisco Unified CME license:

```
se-10-0-0-0> show software licenses

Core:
- application mode: CCME
- total usable system ports: 8

Voicemail/Auto Attendant:
- max system mailbox capacity time: 6000
- max general delivery mailboxes: 15
- max personal mailboxes: 50

Languages:
- max installed languages: 1
- max enabled languages: 1
```

- Calls can be successfully completed between phones on the same Cisco Unified CME router.
- Dial plan for Meet-Me Conferencing is defined. For information, see Dial Plan, on page 1376.

Restriction

- The number of meet-me conferences and parties per conference is limited by the number of DSP resources and number of voice ports available to handle callers.
- There is no set maximum for the number of parties per conference. However, since only the three loudest parties on a multicast conference can be heard, we recommend that the maximum number of parties per conference be limited to eight.
- Only a minimal set of features are provided. Conference bridges can be accessed by any user knowing the correct number to dial (internal or external) with no option to set a password. Callers entering a Meet-Me conference though Cisco Unity Express auto-attendant application are prompted to record their name for playback to all callers on the bridge. No exit tone is played when users leave a conference, nor can a Meet-Me bridge be reserved for use at a future time or date.

Examples

The following partial output from the **show running-config** command shows the configuration on a Cisco 2821 router with Cisco Unified CME and Cisco Unity Express, with comments describing the configuration for setting up Meet-Me Conferencing.

```
Router# show running-config
building configuration...
.
.
.
.
.
!
!---Two T1 ports connected back-to-back to bridge VOIP to Multicast
controller T1 0/3/0
 framing esf
 linecode b8zs
ds0-group 1 timeslots 1 type e&-immediate-start
ds0-group 2 timeslots 2 type e&-immediate-start
ds0-group 3 timeslots 3 type e&-immediate-start
ds0-group 4 timeslots 4 type e&-immediate-start
ds0-group 5 timeslots 5 type e&-immediate-start
ds0-group 6 timeslots 6 type e&-immediate-start
ds0-group 7 timeslots 7 type e&-immediate-start
ds0-group 8 timeslots 8 type e&-immediate-start
ds0-group 9 timeslots 9 type e&-immediate-start
ds0-group 10 timeslots 10 type e&-immediate-start
ds0-group 11 timeslots 11 type e&-immediate-start
ds0-group 12 timeslots 12 type e&-immediate-start
ds0-group 13 timeslots 13 type e&-immediate-start
ds0-group 14 timeslots 14 type e&-immediate-start
ds0-group 15 timeslots 15 type e&-immediate-start
ds0-group 16 timeslots 16 type e&-immediate-start
ds0-group 17 timeslots 17 type e&-immediate-start
ds0-group 18 timeslots 18 type e&-immediate-start
ds0-group 19 timeslots 19 type e&-immediate-start
ds0-group 20 timeslots 20 type e&-immediate-start
ds0-group 21 timeslots 21 type e&-immediate-start
ds0-group 22 timeslots 22 type e&-immediate-start
ds0-group 23 timeslots 23 type e&-immediate-start
ds0-group 24 timeslots 24 type e&-immediate-start
!
controller T1 0/3/1
 framing esf
 clock source internal
 linecode b8zs
```

```
ds0-group 1 timeslots 1 type e&-immediate-start
ds0-group 2 timeslots 2 type e&-immediate-start
ds0-group 3 timeslots 3 type e&-immediate-start
ds0-group 4 timeslots 4 type e&-immediate-start
ds0-group 5 timeslots 5 type e&-immediate-start
ds0-group 6 timeslots 6 type e&-immediate-start
ds0-group 7 timeslots 7 type e&-immediate-start
ds0-group 8 timeslots 8 type e&-immediate-start
ds0-group 9 timeslots 9 type e&-immediate-start
ds0-group 10 timeslots 10 type e&-immediate-start
ds0-group 11 timeslots 11 type e&-immediate-start
ds0-group 12 timeslots 12 type e&-immediate-start
ds0-group 13 timeslots 13 type e&-immediate-start
ds0-group 14 timeslots 14 type e&-immediate-start
ds0-group 15 timeslots 15 type e&-immediate-start
ds0-group 16 timeslots 16 type e&-immediate-start
ds0-group 17 timeslots 17 type e&-immediate-start
ds0-group 18 timeslots 18 type e&-immediate-start
ds0-group 19 timeslots 19 type e&-immediate-start
ds0-group 20 timeslots 20 type e&-immediate-start
ds0-group 21 timeslots 21 type e&-immediate-start
ds0-group 22 timeslots 22 type e&-immediate-start
ds0-group 23 timeslots 23 type e&-immediate-start
ds0-group 24 timeslots 24 type e&-immediate-start
!
!
!
```

!--- Disable keepalive packet to multicast network on voice class and apply to LMR port

```
!
voice class permanent 1
 signal timing oos restart 50000
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
```

!---Loopback0 used as source for all H323 and SCCP packets generated by CME

```
interface Loopback0
 ip address 11.1.1.1 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 11.1.1.1
!
```

!---Vif1 (virtual host interface) used as source for all multicast packets generated by CME

```
!
interface Vif1
 ip address 192.168.11.1 255.255.255.252
 ip pim dense-mode
!
interface FastEthernet0/0
 no ip address
 shutdown
!
```

!---Service-engine interface used to access Cisco Unity Express

```
!
interface Service-Engine0/0
 ip unnumbered Vlan10
service-module ip address 192.168.1.2 255.255.255.0
service-module ip default-gateway 192.168.1.1
!
interface FastEthernet0/1
no ip address
shutdown
!
interface FastEthernet0/0/0
 switchport access vlan 10
 no ip address
!
interface FastEthernet0/0/1
 switchport access vlan 10
 no ip address
!
interface FastEthernet0/0/2
 switchport access vlan 10
```

```
 no ip address
!
interface FastEthernet0/0/3
 switchport access vlan 10
 no ip address
!
interface Vlan1
 no ip address
!
!---All IP phones reside on VLAN 10
interface Vlan10
 ip address 192.168.1.1 255.255.255.0
 ip pim dense-mode
!
 ip classless
!--- Static route to reach other devices on network
ip route 0.0.0.0 0.0.0.0 192.168.1.2
!--- Static route to reach Cisco Unity Express
ip route 192.168.1.2 255.255.255.255 Service-Engine0/0
!
ip http server
ip http path flash:
!
!
tftp-server flash:P00305000301.sbn
!
control-plane
!
!
!
!---VOIP side of the Back-to-Back T1 used for bridging VOIP to
!---Multicast (Hoot n' Holler)
!---Port 0/3/0:x connects to Port 0/3/1:x
voice-port 0/3/0:1
 auto-cut-through
!
voice-port 0/3/0:2
 auto-cut-through
!
.
.
.
!
voice-port 0/3/0:24
 auto-cut-through
!
!---Multicast side of the Back-to-Back T1 used for bridging VOIP to
!---Multicast (Hoot n' Holler)
!--- Port 0/3/1:1 - 8 is permanently trunked to multicast bridge A212
!--- Port 0/3/1:9 - 16 is permanently trunked to multicast bridge A213
!--- Port 0/3/1:17 - 24 is permanently trunked to multicast bridge A214
voice-port 0/3/1:1
 auto-cut-through
 timeouts call-disconnect 3
 connection trunk A212
!
.
.
.
!
voice-port 0/3/1:9
 auto-cut-through
 timeouts call-disconnect 3
 connection trunk A213
!
.
.
.
!
voice-port 0/3/1:17
```

```
 auto-cut-through
 timeouts call-disconnect 3
 connection trunk A214
.
.
.
!
```

!--- Analog FXO lines on port 0/2/x route incoming calls to CUE AA external extension 203

```
voice-port 0/2/0
 connection plar opx 203
!
voice-port 0/2/1
 connection plar opx 203
!
voice-port 0/2/2
 connection plar opx 203
!
voice-port 0/2/3
 connection plar opx 203
!
```

!--- LMR devices are connected to E& ports 0/1/x. The E& ports are permanently trunked to multicast conference bridges. Port 0/1/0 will send and receive audio from conference A212 and port 0/1/1 will send and receive audio from conference A213.

```
voice-port 0/1/0
 voice-class permanent 1
 lmr m-lead audio-gate-in
 lmr e-lead voice
 auto-cut-through
 operation 4-wire
 type 3
 signal lmr
 timeouts call-disconnect 3
 connection trunk A212
!
voice-port 0/1/1
 voice-class permanent 1
 lmr m-lead audio-gate-in
 lmr e-lead voice
 auto-cut-through
 operation 4-wire
 type 3
 signal lmr
 timeouts call-disconnect 3
 connection trunk A213
!
```

!--- Dial-peers to route extension 212 to T1 loopback, which is trunked to bridge A212

```
dial-peer voice 1 pots
 preference 1
 destination-pattern 212
 port 0/3/0:1
!
.
.
.
!
dial-peer voice 8 pots
 preference 8
 destination-pattern 212
 port 0/3/0:8
!
```

!--- Dial-peers to route extension 213 to T1 loopback, which is trunked to bridge A213

```
dial-peer voice 9 pots
 preference 1
 destination-pattern 213
 port 0/3/0:9
!
.
.
.
!
dial-peer voice 16 pots
```

```
 preference 8
 destination-pattern 213
 port 0/3/0:16
!
!--- Dial-peers to route extension 214 to T1 loopback, which is trunked to bridge A214
dial-peer voice 17 pots
 preference 1
 destination-pattern 214
 port 0/3/0:17
!
.
.
.
!
dial-peer voice 24 pots
 preference 8
 destination-pattern 214
 port 0/3/0:24
!--- Dial-peer to route calls to CUE AA for internal ext. 202 and external ext. 203
dial-peer voice 200 voip
 destination-pattern 20.
 session protocol sipv2
 session target ipv4:192.168.1.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
!--- Dial-peers for multicast bridges
dial-peer voice 212 voip
 destination-pattern A212
 voice-class permanent 1
 session protocol multicast

 session target ipv4:237.111.0.0:22222
 dtmf-relay cisco-rtp
 codec g711ulaw
 vad aggressive
!
dial-peer voice 213 voip
 destination-pattern A213
 voice-class permanent 1
 session protocol multicast
 session target ipv4:237.111.0.1:22222
 dtmf-relay cisco-rtp
 codec g711ulaw
 vad aggressive
!
dial-peer voice 214 voip
 destination-pattern A214
 voice-class permanent 1
 session protocol multicast
 session target ipv4:237.111.0.2:22222
 dtmf-relay cisco-rtp
 codec g711ulaw
 vad aggressive
!
telephony-service
 load 7960-7940 P00305000301
 max-ephones 24
 max-dn 144
 ip source-address 11.1.1.1 port 2000
  create cnf-files version-stamp Jan 01 2002 00:00:00
 voicemail 200
 web admin system name cisco password cisco
 max-conferences 8 gain -6
 transfer-system full-consult
!
!
ephone-dn 1 dual-line
 number 150
!
.
```

.
.

What to Do Next

Load and configure the auto-attendant script file for Meet-me Conferencing. For information about logging into and GUI windows and menus, see Cisco Unity Express GUI Administrator Guide.

Step 1 Go to the Download Software site. Download the Conference Express TCL and AA voice files (conf-express.zip). Unzip the archive to a folder on your PC.

Step 2 Log into Cisco Unity Express as administrator.

Step 3 Navigate to the **Voice mail** > **Auto Attendant** menu and click **Add**. The **Add a New Automated Attendant** window appears.

Step 4 In the Select Automated Attendant area, configure the parameters listed in the following table. Enter the required information in the corresponding field.

Parameter Name	Value
Select Automated Attendant Script	mp-exp.aef
Application Name (lower case)	conference-express
Destination file name	mp-exp.aef

Step 5 Click **Next**. The **Upload** window appears.

Step 6 Upload the script (mp-exp.aef) from your PC to the auto-attendant application. For information, see online help.

Step 7 On the Add a New Automated Attendant window, configure parameters with numbers as defined in your dial plan and with the values listed in following table. Enter the required information in the corresponding field. For dial plan information, see Dial Plan, on page 1376.

Field Name	Value
Script Parameters	
BridgeDir	bridge.wav
record_name	record_name.wav
SystemProblems	SystemProblems.wav
Call Handling	
Call-in Number	InternalNumber as defined in dial plan

Field Name	Value
Maximum Sessions	4

Step 8 Click **Finish**.

Step 9 Navigate to the **Administration** > **Call-In Numbers** menu and click **Add**.

Step 10 On the **Add a Call-In Number** window, configure the parameters listed in the following table. Enter the required information in the corresponding field.

Field Name	Value
Application	conference-express
Call-in Number	ExternalNumber as defined in dial plan
Maximum Sessions	4

Step 11 Click **Add**.

Step 12 Confirm that two call-in numbers for the conference-express application are enabled on the **Administration** > **Call-In Numbers** window.

Configuration Examples for Conferencing

Example for Configuring Basic Conferencing

The following example sets the maximum number of conferences for a Cisco Unified IP phone to 4 and configures a gain of 6 db for inbound audio packets from remote PSTN or VoIP calls joining a conference:

```
telephony-service
max-conferences 4 gain 6
```

Example for Configuring End of Conference Options

In the following example, extension 3555 initiates a three-way conference. After the conference is established, extension 3555 can press the Confrn soft key to disconnect the last party that was connected and remain connected to the first party that was connected. If extension 3555 hangs up from the conference, the other two parties remain connected if one of them is local to the Cisco Unified CME system.

```
ephone-dn 35
 number 3555

ephone 24
 button 1:35
```

```
keep-conference drop-last local-only
```

In the following example, extension 3666 initiates a three-way conference. After the conference is established, extension 3666 can press the Confrn soft key to disconnect the last party that was connected and remain connected to the first party that was connected. Also, extension 3666 can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected.

```
ephone-dn 36
 number 3666

ephone 25
 button 1:36
 keep-conference drop-last endcall
```

In the following example, extension 3777 initiates a three-way conference. After the conference is established, extension 3777 can press the Confrn soft key to disconnect the last party that was connected and remain connected to the first party that was connected. Also, extension 3777 can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected *only* if one of the two parties is local to the Cisco Unified CME system.

```
ephone-dn 38
 number 3777

ephone 27
 button 1:38
 keep-conference drop-last endcall local-only
```

In the following example, extension 3999 initiates a three-way conference. After the conference is established, extension 3999 can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected *only* if one of the two parties is local to the Cisco Unified CME system. Extension 3999 can also use the Confrn soft key to break up the conference but stay connected to both parties.

```
ephone-dn 39
 number 3999

ephone 29
 button 1:39
 keep-conference endcall local-only
```

Example for Keep-Conference on SIP Phones

In the following example, extension 3555 initiates a three-way conference on SIP phones using keep-conference configured under **voice register pool** .

```
voice register dn 35
  number 3555

voice register pool 24
  number 1 dn 35
  keep-conference
```

Following is a sample configuration for keep-conference under **voice register template**.

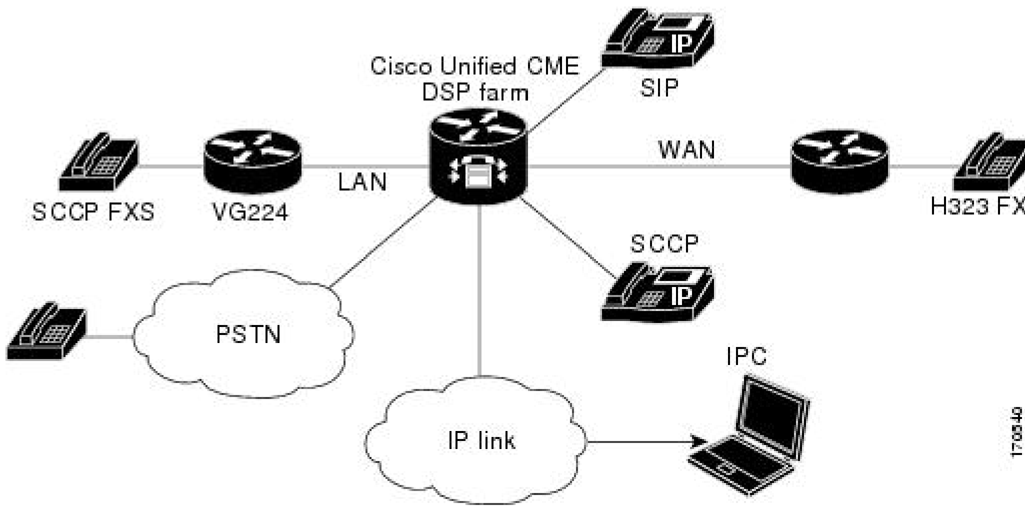
```
voice register template 24
  keep-conference

voice register pool 35
```

```
template 24
```

Example of DSP Farm and Cisco Unified CME on the Same Router

In this example, the DSP farm and Cisco Unified CME are on the same router as shown in Figure 67: CME and the DSP Farm on the Same Router, on page 1408.

Figure 67: CME and the DSP Farm on the Same Router




```
    Current configuration : 16345 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
service internal
!
hostname cmedsprtr
!
boot-start-marker
boot-end-marker
!
logging buffered 90000 debugging
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip cef
!
!
ip dhcp pool phone1
 host 10.4.188.66 255.255.0.0
 client-identifier 0100.0ab7.b144.4a
 default-router 10.4.188.65
 option 150 ip 10.4.188.65
!
ip dhcp pool phone2
 host 1.4.188.67 255.255.0.0
 client-identifier 0100.3094.c269.35
```

```
 default-router 10.4.188.65
 option 150 ip 10.4.188.65
!
!
voice-card 1
 dsp services dspfarm
!
!
voice call send-alert
voice call carrier capacity active
!
voice service voip
 allow-connections h323 to h323
 supplementary-service h450.12
 h323
!
!
!
!
controller E1 1/0
 framing NO-CRC4
!
controller E1 1/1
!
!
interface FastEthernet0/0
 ip address 10.4.188.65 255.255.0.0
 duplex auto
 speed auto
 no keepalive
 no cdp enable
 no clns route-cache
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 no clns route-cache
!
ip route 10.4.0.0 255.255.0.0 FastEthernet0/0
ip route 192.168.254.254 255.255.255.255 10.4.0.1
!
ip http server
!
!
control-plane
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.188.65 identifier 1 version 4.0
sccp
!
sccp ccm group 123
 associate ccm 1 priority 1
 associate profile 1 register mtp00097c5e9ce0
 keepalive retries 5
!
!
dspfarm profile 1 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 6
 associate application SCCP
!
dial-peer cor custom
!
!
!
```

```
 dial-peer voice 6 voip
  destination-pattern 6...
  session target ipv4:10.4.188.90
 !
 telephony-service
  conference hardware
  load 7960-7940 P00307020400
  load 7905 CP7905060100SCCP050309A.sbin
  max-ephones 48
  max-dn 180
  ip source-address 10.4.188.65 port 2000
  timeouts ringing 500
  system message MY MELODY (2611)
  sdspfarm units 4
  sdspfarm tag 1 mtp00097c5e9ce0
  max-conferences 4 gain -6
  call-forward pattern ....
  transfer-system full-consult
  transfer-pattern 7...
  transfer-pattern ....
  create cnf-files version-stamp Jan 01 2002 00:00:00
 !
 !
 ephone-template 1
  softkeys hold Newcall Resume Select Join
  softkeys idle Cfwdall ConfList Dnd Gpickup HLog Join Login Newcall Pickup Redial RmLstC
  softkeys seized Redial Pickup Gpickup HLog Meetme Endcall
  softkeys connected Acct ConfList Confrn Endcall Flash HLog Hold Join Park RmLstC Select
Trnsfer
 !
 !
 ephone-dn 1 dual-line
  number 8001
  name melody-8001
 !
 !
 ephone-dn 2 dual-line
  number 8002
 !
 !
 ephone-dn 3 dual-line
  number 8003
 !
 !
 ephone-dn 4 dual-line
  number 8004
 !
 !
 ephone-dn 5 dual-line
  number 8005
 !
 !
 ephone-dn 6 dual-line
  number 8006
 !
 !
 ephone-dn 7 dual-line
  number 8007
 !
 !
 ephone-dn 8 dual-line
  number 8008
 !
 !
 ephone-dn 60 dual-line
  number 8887
  conference meetme
  no huntstop
 !
 !
 ephone-dn 61 dual-line
  number 8887
  conference meetme
```

```
 preference 1
 no huntstop
!
!
ephone-dn 62 dual-line
 number 8887
 conference meetme
 preference 2
 no huntstop
!
!
ephone-dn 63 dual-line
 number 8887
 conference meetme
 preference 3
!
!
ephone-dn 64 dual-line
 number 8889
 name Conference
 conference ad-hoc
 no huntstop
!
!
ephone-dn 65 dual-line
 number 8889
 name Conference
 conference ad-hoc
 preference 1
 no huntstop
!
!
ephone-dn 66 dual-line
 number 8889
 name Conference
 conference ad-hoc
 preference 2
 no huntstop
!
!
ephone-dn 67 dual-line
 number 8889
 name Conference
 conference ad-hoc
 preference 3
!
!
ephone 1
 ephone-template 1
 mac-address 0030.94C2.6935
 type 7960
 button 1:1 2:2
!
!
ephone 2
 ephone-template 1
 mac-address 000A.B7B1.444A
 type 7940
 button 1:4 2:8
!
line con 0
 exec-timeout 0 0
line aux 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 login
line vty 5 15
 login
!
!
end
```

The following is an example of DSP Farm and Unified CME on the same router for SIP Phones.

```
Current configuration : 10821 bytes
!
version 16.5
service timestamps debug datetime msec
service timestamps log datetime msec
service sequence-numbers
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
 address-family ipv6
exit-address-family
!
! card type command needed for slot/bay 0/1
no logging queue-limit
logging buffered 100000000
no logging rate-limit
no logging console
!
no aaa new-model
!
!
ipv6 unicast-routing
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
voice service voip
no ip address trusted authenticate
media disable-detailed-stats
allow-connections sip to sip
no supplementary-service sip refer
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
sip
  registrar server expires max 240 min 60
!
!
voice register global
mode cme
source-address 8.39.23.16 port 5060
no privacy
timeouts interdigit 30
max-dn 40
max-pool 40
voicemail 9000
tftp-path flash:
create profile sync 0095202153430137
conference hardware
!
voice register dn  1
number 1001
name SIP Ph 1
!
voice register dn  2
number 1002
name SIP Ph 2
!
voice register dn  3
number 1003
name SIP Ph 3
!
```

```
voice register template  1
softkeys idle  HLog Mobility Newcall Pickup Redial
softkeys ringIn  Answer DND
softkeys connected  ConfList Confrn Endcall Hold Mobility Park Trnsfer
softkeys remote-in-use  Barge Newcall cBarge
!
voice register pool  1
busy-trigger-per-button 10
id mac B000.B4BA.F3DA
type 8851
number 1 dn 1
template 1
dtmf-relay rtp-nte
username xxxx password xxxx
codec g711ulaw
no vad
!
voice register pool  2
busy-trigger-per-button 10
id mac 1CE8.5DC9.C054
type 8851
number 1 dn 2
template 1
dtmf-relay rtp-nte
username xxxx password xxxx
codec g711ulaw
no vad
!
voice register pool  3
busy-trigger-per-button 10
id mac 00AF.1F9D.FB9F
type 8841
number 1 dn 3
template 1
dtmf-relay rtp-nte
username xxxx password xxxx
codec g711ulaw
no vad
!
!
voice translation-rule 1
rule 1 /^1234/ /301/
!
voice translation-rule 4
rule 4 /^1(..)$/ /51237812\1/
!
!
voice translation-profile PSTN_Callforwarding
translate redirect-target 4
!
voice translation-profile cmein
translate called 1
!
!
voice-card 0/1
dsp services dspfarm
!
restconf
!
username xxxx password xxxx
!
redundancy
mode none
!
!
threat-visibility
!
!
interface GigabitEthernet0/0/0
ip address 8.39.23.16 255.255.0.0
negotiation auto
!
interface GigabitEthernet0/0/1
```

```
ip address 10.64.86.106 255.255.0.0
shutdown
media-type rj45
negotiation auto
ipv6 address 2001:420:54FF:13::312:55/119
ipv6 enable
!
interface GigabitEthernet0/0/2
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/0/3
no ip address
shutdown
negotiation auto
!
interface Service-Engine0/1/0
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
shutdown
negotiation auto
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http secure-port 8443
ip tftp source-interface GigabitEthernet0/0/1
ip tftp blocksize 8192
ip dns server
ip rtcp report interval 65535
ip route 0.0.0.0 0.0.0.0 8.39.0.1
ip route 8.0.0.0 255.0.0.0 8.39.0.1
ip route 202.153.144.0 255.255.255.0 8.39.0.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
!
!
tftp-server bootflash
tftp-server flash:vc488xx.12-0-1MN-113.sbn
tftp-server flash:sip88xx.12-0-1MN-113.loads
tftp-server flash:sb288xx.BE-01-020.sbn
tftp-server flash:kern88xx.12-0-1MN-113.sbn
tftp-server flash:fbi88xx.BE-01-010.sbn
tftp-server flash:rootfs88xx.12-0-1MN-113.sbn
!
!
ipv6 access-list preauth_v6
permit udp any any eq domain
permit tcp any any eq domain
permit icmp any any nd-ns
permit icmp any any nd-na
permit icmp any any router-solicitation
permit icmp any any router-advertisement
permit icmp any any redirect
permit udp any eq 547 any eq 546
permit udp any eq 546 any eq 547
deny ipv6 any any
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
```

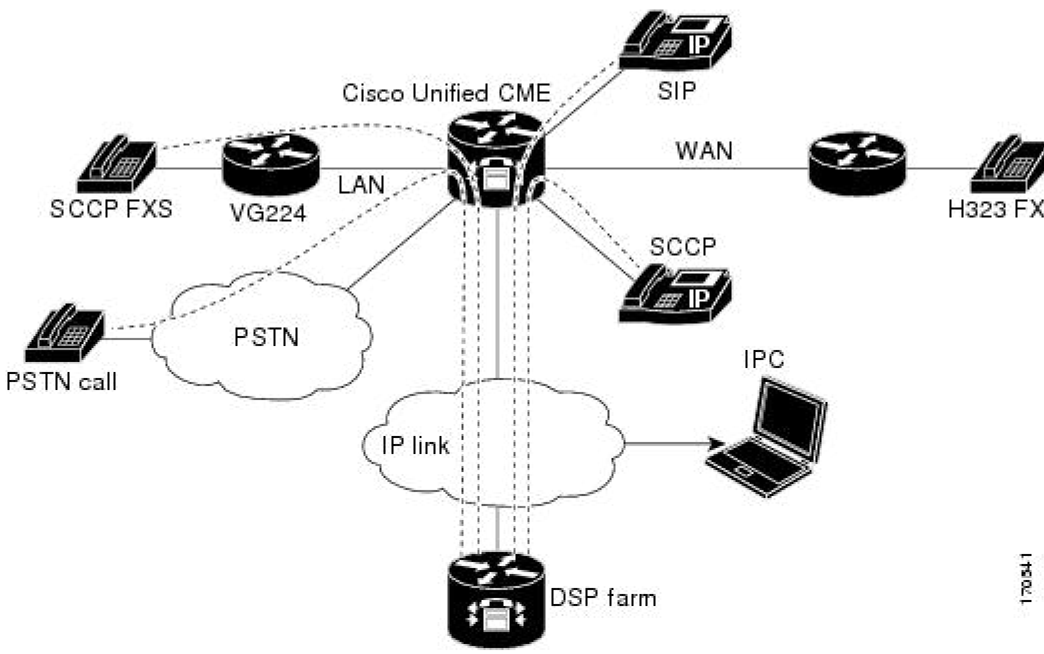
```
!
sccp local GigabitEthernet0/0/0
sccp ccm 8.39.23.16 identifier 1 version 7.0
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register conf-moto
!
!
!
telephony-service
sdspfarm units 2
sdspfarm tag 1 conf-moto
no privacy
conference hardware
no auto-reg-ephone
max-ephones 40
max-dn 40
ip source-address 8.39.23.16 port 2000
service phone sshAccess 0
service phone webAccess 0
service directed-pickup gpickup
max-conferences 8 gain -6
call-park system application
hunt-group logout HLog
moh enable-g711 "flash:/scripts/en_bacd_music_on_hold.au"
transfer-system full-consult
fac standard
create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
dspfarm profile 2 transcode universal
 codec g729abr8
codec g729ar8
codec g711alaw
codec g711ulaw
codec g729br8
maximum sessions 2
associate application CUBE
!
dspfarm profile 1 conference
 codec g729br8
codec g729r8
codec g729abr8
codec g729ar8
codec g711alaw
codec g711ulaw
maximum sessions 2
associate application SCCP
!
dial-peer voice 1 voip
destination-pattern 20..
session protocol sipv2
session target ipv4:8.39.24.41
dtmf-relay rtp-nte
!
!
gateway
 media-inactivity-criteria all
timer receive-rtcp 1000
timer receive-rtp 1200
!
sip-ua
 mwi-server ipv4:8.41.24.7 expires 3600 port 5060 transport udp unsolicited
presence enable
!
!
ephone-dn  1  octo-line
number 1006
!
!
ephone-dn  2  octo-line
```

```
number 1007
!
!
ephone-dn  3  octo-line
number 1008
!
!
ephone-dn  4  octo-line
number 1009
!
!
ephone-dn  5  octo-line
number A001
conference ad-hoc
!
!
ephone-dn  6  octo-line
number A002
conference ad-hoc
!
!
ephone  1
device-security-mode none
mac-address 9876.0000.0006
type 7975
button  1:1
!
!
!
ephone  2
device-security-mode none
mac-address 9876.0000.0007
type 7975
button  1:2
!
!
!
ephone  3
device-security-mode none
mac-address 9876.0000.0008
type 7975
button  1:3
!
!
!
ephone  4
device-security-mode none
mac-address 9876.0000.0009
type 7975
button  1:4
!
!
alias exec poolall show voice register pool all brief
!
line con 0
transport input none
stopbits 1
speed 115200
line aux 0
stopbits 1
line vty 0 4
password xxxx
login local
transport input telnet
!
no network-clock synchronization automatic
!
end
```

Example of DSP Farm and Cisco Unified CME on Different Routers

In this example, the DSP farm and Cisco Unified CME are on different routers as shown in Figure 68: Cisco Unified CME and the DSP Farm on Different Routers, on page 1417.

Figure 68: Cisco Unified CME and the DSP Farm on Different Routers



This section contains configuration examples for the following routers:

• Example of Cisco Unified CME Router Configuration, on page 1417
• Example of DSP Farm Router Configuration, on page 1423

Example of Cisco Unified CME Router Configuration

```
Current configuration : 5659 bytes
!
version 12.4
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption
!
boot-start-marker
boot-end-marker
!
!
card type command needed for slot 1
logging buffered 3000000 debugging
!
no aaa new-model
!
resource policy
!
```

```
no network-clock-participate slot 1
no network-clock-participate aim 0
!
voice-card 1
 no dspfarm
!
voice-card 3
 dspfarm
!
ip cef
!
!
no ip dhcp use vrf connected
!
ip dhcp pool IPPhones
 network 10.15.15.0 255.255.255.0
 option 150 ip 10.15.15.1
 default-router 10.15.15.1
!
!
interface FastEthernet0/0
 ip address 10.3.111.102 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 10
 ip address 10.15.14.1 255.255.255.0
!
interface FastEthernet0/1.2
 encapsulation dot1Q 20
 ip address 10.15.15.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.5.51.1
ip route 0.0.0.0 0.0.0.0 10.3.0.1
!
ip http server
!
!
!
!
control-plane!
!
!
!
dial-peer voice 1 voip
 destination-pattern 3...
 session target ipv4:10.3.111.101
!
!
telephony-service
 conference hardware
 load 7910 P00403020214
 load 7960-7940 P003-07-5-00
 max-ephones 50
 max-dn 200
 ip source-address 10.15.15.1 port 2000
 sdspfarm units 4
 sdspfarm transcode sessions 12
 sdspfarm tag 1 confer1
 sdspfarm tag 4 xcode1
 max-conferences 8 gain -6
 moh flash:music-on-hold.au
 multicast moh 239.0.0.0 port 2000
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
```

```
ephone-template 1
 softkeys hold Resume Newcall Select Join
 softkeys idle Redial Newcall ConfList RmLstC Cfwdall Join Pickup Login HLog Dnd Gpickup
 softkeys seized Endcall Redial Cfwdall Meetme Pickup Callback
 softkeys alerting Endcall Callback
 softkeys connected Hold Endcall Confrn Trnsfer Select Join ConfList RmLstC Park Flash !
ephone-dn 1 dual-line
 number 6000
!
!
ephone-dn 2 dual-line
 number 6001
!
!
ephone-dn 3 dual-line
 number 6002
!
!
ephone-dn 4 dual-line
 number 6003
!
!
ephone-dn 5 dual-line
 number 6004
!
!
ephone-dn 6 dual-line
 number 6005
!
!
ephone-dn 7 dual-line
 number 6006
!
!
ephone-dn 8 dual-line
 number 6007
!
!
ephone-dn 9 dual-line
 number 6008
!
!
ephone-dn 10 dual-line
 number 6009
!
!
ephone-dn 11
 number 6011
!
!
ephone-dn 12
 number 6012
!
!
ephone-dn 13
 number 6013
!
!
ephone-dn 14
 number 6014
!
!
ephone-dn 15
 number 6015
!
!
ephone-dn 16
 number 6016
!
!
ephone-dn 17
 number 6017
!
```

```
!
ephone-dn 18
 number 6018
!
!
ephone-dn 19
 number 6019
!
!
ephone-dn 20
 number 6020
!
!
ephone-dn 21
 number 6021
!
!
ephone-dn 22
 number 6022
!
!
ephone-dn 23
 number 6023
!
!
ephone-dn 24
 number 6024
!
!
ephone-dn 25 dual-line
 number 6666
 conference meetme
 preference 1
 no huntstop
!
!
ephone-dn 26 dual-line
 number 6666
 conference meetme
 preference 2
 no huntstop
!
!
ephone-dn 27 dual-line
 number 6666
 conference meetme
 preference 3
 no huntstop
!
!
ephone-dn 28 dual-line
 number 6666
 conference meetme
 preference 4
 no huntstop
!
!
ephone-dn 29 dual-line
 number 8888
 conference meetme
 preference 1
 no huntstop
!
!
ephone-dn 30 dual-line
 number 8888
 conference meetme
 preference 2
 no huntstop
!
!
ephone-dn 31 dual-line
 number 8888
```

```
 conference meetme
 preference 3
 no huntstop
!
!
ephone-dn 32 dual-line
 number 8888
 conference meetme
 preference 4
!
!
ephone-dn 33
 number 6033
!
!
ephone-dn 34
 number 6034
!
!
ephone-dn 35
 number 6035
!
!
ephone-dn 36
 number 6036
!
!
ephone-dn 37
 number 6037
!
!
ephone-dn 38
 number 6038
!
!
ephone-dn 39
 number 6039
!
!
ephone-dn 40
 number 6040
!
!
ephone-dn 41 dual-line
 number 6666
 conference meetme
 preference 5
 no huntstop
!
!
ephone-dn 42 dual-line
 number 6666
 conference meetme
 preference 6
 no huntstop
!
!
ephone-dn 43 dual-line
 number 6666
 conference meetme
 preference 7
 no huntstop
!
!
ephone-dn 44 dual-line
 number 6666
 conference meetme
 preference 8
 no huntstop
!
!
ephone-dn 45 dual-line
 number 6666
```

```
 conference meetme
 preference 9
 no huntstop
!
!
ephone-dn 46 dual-line
 number 6666
 conference meetme
 preference 10
 no huntstop
!
!
ephone-dn 47 dual-line
 number 6666
 conference meetme
 preference 10
 no huntstop
!
!
ephone-dn 48 dual-line
 number 6666
 conference meetme
 preference 10
!
!
ephone-dn 51 dual-line
 number A0001
 name conference
 conference ad-hoc
 preference 1
 no huntstop
!
!
ephone-dn 52 dual-line
 number A0001
 name conference
 conference ad-hoc
 preference 2
 no huntstop
!
!
ephone-dn 53 dual-line
 number A0001
 name conference
 conference ad-hoc
 preference 3
 no huntstop
!
!
ephone-dn 54 dual-line
 number A0001
 name conference
 conference ad-hoc
 preference 4
!
!
ephone 1
 ephone-template 1
 mac-address C863.B965.2401
 type anl
 button 1:1
!
!
!
ephone 2
 ephone-template 1
 mac-address 0016.C8BE.A04A
 type 7920
!
!
!
ephone 3
 ephone-template 1
```

```
 mac-address C863.B965.2400
 type anl
 button 1:2
!
!
!
ephone 4
 no multicast-moh
 ephone-template 1
 mac-address 0017.952B.7F5C
 type 7912
 button 1:4
!
!
!
ephone 5
 ephone-template 1
 ephone 6
 no multicast-moh
 ephone-template 1
 mac-address 0017.594F.1468
 type 7961GE
 button 1:6
!
!
!
ephone 11
 ephone-template 1
 mac-address 0016.C8AA.C48C
 button 1:10 2:15 3:16 4:17
 button 5:18 6:19 7:20 8:21
 button 9:22 10:23 11:24 12:33
 button 13:34 14:35 15:36 16:37
 button 17:38 18:39 19:40
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Example of DSP Farm Router Configuration

```
    Current configuration : 2179 bytes
!
! Last configuration change at 05:47:23 UTC Wed Jul 12 2006
!
version 12.4
service timestamps debug datetime msec localtime
no service timestamps log uptime
no service password-encryption
hostname dspfarmrouter
!
boot-start-marker
boot-end-marker
!
!
card type command needed for slot 1
logging buffered 4096 debugging enable password lab
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
!
!
```

```
ip cef
!
!
no ip domain lookup
!
!
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
 dsp services dspfarm

interface GigabitEthernet0/0
 ip address 10.3.111.100 255.255.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.1
 encapsulation dot1Q 100
 ip address 192.168.1.10 255.255.255.0
!
interface GigabitEthernet0/1.2
 encapsulation dot1Q 200
 ip address 192.168.2.10 255.255.255.0
!
interface GigabitEthernet0/1.3
 encapsulation dot1Q 10
 ip address 10.15.14.10 255.255.255.0
!
interface GigabitEthernet0/1.4
 encapsulation dot1Q 20
 ip address 10.15.15.10 255.255.255.0 !
ip route 10.0.0.0 255.0.0.0 10.3.0.1
ip route 192.168.0.0 255.0.0.0 10.3.0.1
!
!
ip http server
!
!
!
!
control-plane
!
sccp local GigabitEthernet0/0
sccp ccm 10.15.15.1 identifier 1 version 4.1
!
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 101 register confer1
 associate profile 103 register xcode1
!
!
dspfarm profile 103 transcode
 codec g711ulaw
 codec g711alaw
 codec g729r8
 maximum sessions 6
 associate application SCCP
!
dspfarm profile 101 conference
 codec g711ulaw
 codec g711alaw
 codec g729r8
 maximum sessions 5
 associate application SCCP
!
!
!
!
line con 0
 exec-timeout 0 0
```

```
line aux 0
line vty 0 4
 session-timeout 300
 exec-timeout 0 0
 password
 no login
!
scheduler allocate 20000 1000
!
end
```

Where to Go Next

Controlling Use of the Conference Soft Key

To block the functioning of the conference (Confrn) soft key without removing the key display, create and apply an ephone template that contains the **features blocked** command. For more information, see Templates, on page 1427.

To remove the conference (Confrn) soft key from one or more phones, create and apply an ephone template that contains the appropriate **softkeys** command. For more information, see Customize Softkeys, on page 925.

Feature Information for Conferencing

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

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

Table 109: Feature Information for Conferencing

Feature Name	Cisco Unified CME Version	Feature Information
Meet-me Conference	11.7	Added support for hardware-based Meet-me Conference on Cisco 4000 Series Integrated Services Router.
	4.1	Added support for hardware-based meet-me conferences created by parties calling a designated conference number.

Feature Name	Cisco Unified CME Version	Feature Information
Multi-party Ad Hoc Conference	11.7	Added support for hardware-based Multi-party Conference on Cisco 4000 Series Integrated Services Router.
	4.1	Added support for hardware-based Multi-party Conferencing Enhancements which uses DSPs to enhance ad hoc conferencing by allowing more parties than software-based ad hoc conferencing. Configuring multi-party ad hoc conferencing disables three-party ad hoc conferencing.
Three-Party Ad Hoc Conference	11.7	Added support for three-party Ad Hoc conference on Cisco 4000 Series Integrated Services Router.
	4.0	• End-of-conference options were introduced. • Phones connected in a three-way conference display "Conference."
	3.2.2	Conference gain control for external calls was introduced.
	3.2	Conference initiator drop-off control was introduced.
	2.0	Support for software-based conferencing was introduced.

CHAPTER 47

Templates

Information About Templates

Phone Templates

An ephone or voice-register template is a set of features that can be applied to one or more individual phones using a single command.

Ephone templates were introduced in Cisco CME 3.2 to manipulate softkey display and order on IP phones.

In Cisco Unified CME 4.0, ephone templates were significantly enhanced to include a number of additional phone features. Templates allow you to uniformly and easily implement the features you select for a set of phones. A maximum of 20 ephone templates can be created in a Cisco Unified CME system, although an ephone can have only one template applied to it at a time.

In Cisco Unified CME 4.3 and later versions, an ephone template cannot be applied to a particular phone unless its configuration file includes its Mac address. If you attempt to apply a template to a phone for which the MAC address in not configured, a message appears.

If you use an ephone template to apply a command to a phone and you also use the same command in ephone configuration mode for the same phone, the value set in ephone configuration mode has priority.

Voice-register templates were introduced in Cisco CME 3.4 to enable sets of features to be applied to individual SIP Phones that are connected directly in Cisco Unified CME. Typically, features to be enabled by using a voice-register template are not configurable in other configuration modes. A maximum 10 voice-register templates can be defined in Cisco Unified CME, although a phone can have only one template applied to it at a time.

Type ? in ephone-template or voice-register-template configuration mode to display a list of features that can be implemented by using templates.

For configuration information, see Create an Ephone Template, on page 1428.

Ephone-dn Templates

Ephone-dn templates allow you to apply a standard set of features to ephone-dns. A maximum of 15 ephone-dn templates can be created in a Cisco Unified CME system, although an ephone-dn can have only one template applied to it at a time.

If you use an ephone-dn template to apply a command to an ephone-dn and you also use the same command in ephone-dn configuration mode for the same ephone-dn, the value that you set in ephone-dn configuration mode has priority.

Type ? in ephone-dn-template configuration mode to display a list of features that can be implemented by using templates.

For configuration information, see Create an Ephone-dn Template, on page 1430.

Configure Templates

Create an Ephone Template

To create an ephone template and apply it to a phone, perform the following steps.

Before You Begin

- In Cisco Unified CME 4.3 and later versions, the configuration file for a particular phone must contain its MAC address before an ephone template can be applied to that phone. To explicitly configure a MAC address, use the **mac-address** command in ephone configuration mode. For configuration information, see Configuring Phones to Make Basic Calls, on page 223.
- It is recommended to configure cnf-file per phone before adding ephone-template under ephone.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. *command*
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
8. **restart**
9. **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-template** *template-tag* **Example:** `Router(config)# ephone-template 15`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range is 1 to 20.
Step 4	*command* **Example:** `Router(config-ephone-template)# features blocked Park Trnsfer`	Applies the specified command to the ephone template that is being created. • Type **?** for a list of commands that can be used in this step. Repeat this step for each command that you want to add to the ephone template.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 15`	Applies an ephone template to the ephone that is being configured.
Step 8	**restart** **Example:** `Router(config-ephone)# restart`	Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information. **Note** Restart all ephones using the **restart all** command in telephony-service configuration mode.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Create an Ephone-dn Template

To create an ephone-dn template and apply it to an ephone-dn, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn-template** *template-tag*
4. *command*
5. **exit**
6. **ephone-dn** *dn-tag*
7. **ephone-dn-template** *template-tag*
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	**ephone-dn-template** *template-tag* **Example:** `Router(config)# ephone-dn-template 3`	Enters ephone-dn-template configuration mode to create an ephone-dn template. • *template-tag*—Unique identifier for the ephone-dn template that is being created. Range is 1 to 20.

	Command or Action	Purpose
Step 4	*command* **Example:** `Router(config-ephone-dn-template)# call-forwarding busy 4000`	Applies the specified command to the ephone-dn template that is being created. • Type **?** for a list of commands that can be used in this step. Repeat this step to add more commands to the template.
Step 5	**exit** **Example:** `Router(config-ephone-dn-template)# exit`	Exits ephone-dn-template configuration mode.
Step 6	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 23`	Enters ephone-dn configuration mode. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks.
Step 7	**ephone-dn-template** *template-tag* **Example:** `Router(config-ephone-dn)# ephone-dn-template 3`	Applies an ephone-dn template to the ephone-dn that is being configured.
Step 8	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Verify Templates on SCCP Phones

To view the configuration of a template, and verify to which phone or directory number a template is applied, perform the following steps.

Step 1 **show telephony-service ephone**

Use is command to display information about SCCP phones in Cisco Unified CME, including which template-tags are enabled in the configuration for a phone.

```
Router# show telephony-service ephone 1
ephone-dn-template  1
 description Call Center Line 1
 call-forward busy 500
 call-forward noan 500 timeout 10
 pickup-group 33!
!
```

Step 2 **show telephony-service ephone-template**
Use is command to display information about an ephone template in Cisco Unified CME, including a list of features enabled in the configuration.

Step 3 **show telephony-service ephone-dn**
Use is command to display information about directory numbers, including which template-tags are enabled in the configuration for a directory number.

```
Router# show telephony-service ephone-dn 4
!
ephone-dn  4  dual-line
 number 136
 description Desk4
 ephone-dn template 1
 ephone-hunt login
```

Step 4 **show telephony-service ephone-dn-template**
Use is command to display information about an ephone-dn template in Cisco Unified CME, including a list of features enabled in the configuration.

Create and Apply Templates for SIP Phones

To create templates of common features and softkeys that can be applied to individual Cisco SIP Phones, follow the steps in this section.

Before You Begin

- Cisco CME 3.4 or a later version.
- The **mode** cme command must be enabled in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. *command*
5. **exit**
6. **voice register pool** *pool-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 1`	Enters voice register template configuration mode to define a template of common parameters for SIP phones in Cisco Unified CME. • Range is 1 to 5.
Step 4	*command* **Example:** `Router(config-register-template)# anonymous block`	Applies the specified command to this template and enables the corresponding feature on any supported SIP phone that uses a template in which this command is configure. • Type **?** to display list of commands that can be used in a voice register template. Repeat this step for each feature to be added to this voice register template.
Step 5	**exit** **Example:** `Router(config-register-template)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 6	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 3`	Enters voice register pool configuration mode to set phone-specific parameters for SIP phones. • *pool-tag*—Unique sequence number of the Cisco SIP phone to be configured. Range is 1 to 100 or the upper limit as defined by **max-pool** command.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# voice register pool 1`	Applies a template created with the **voice register template** command. • *template-tag*—Unique sequence number of the template to be applied to the SIP phone specified by the **voice register pool** command. Range is 1 to 5.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows templates 1 and 2 and how to do the following:

- Apply template 1 to SIP phones 1 to 3.
- Apply template 2 to SIP phone 4.
- Remove a previously created template 5 from SIP phone 5.

```
Router(config)# voice register template 1
 Router(config-register-temp)# anonymous block
 Router(config-register-temp)# caller-id block
 Router(config-register-temp)# voicemail 5001 timeout 15

Router(config)# voice register template 2
 Router(config-register-temp)# anonymous block
 Router(config-register-temp)# caller-id block
 Router(config-register-temp)# no conference
 Router(config-register-temp)# no transfer-attended
 Router(config-register-temp)# voicemail 5005 timeout 15

Router(config)# voice register pool 1
 Router(config-register-pool)# template 1

Router(config)# voice register pool 2
 Router(config-register-pool)# template 1

Router(config)# voice register pool 3
 Router(config-register-pool)# template 1

Router(config)# voice register pool 4
 Router(config-register-pool)# template 2

Router(config)# voice register pool 5
 Router(config-register-pool)# no template 5
```

Configuration Examples for Creating Templates

Example to Block The Use of Park and Transfer Soft Keys Using Ephone Template

The following example creates an ephone template to block the use of Park and Transfer soft keys. It is applied to ephone 36 and extension 2333.

```
ephone-template 15
   features blocked Park Trnsfer

  ephone-dn 2
   number 2333

  ephone 36
   button 1:2
   ephone-template 15
```

Example to Set Call Forwarding Using Ephone-dn Template

The following example creates ephone-dn template 3, which sets call forwarding on busy and no answer to forward calls to extension 4000 and sets the pickup group to 4. Ephone-dn template 3 is then applied to ephone-dn 23 and ephone-dn 33, which appear on ephones 13 and 14, respectively.

```
ephone-dn-template 3
   call-forwarding busy 4000
   call-forwarding noan 4000 timeout 30
   pickup group 4

  ephone-dn 23
   number 2323
   ephone-dn-template 3

  ephone-dn 33
   number 3333
   ephone-dn-template 3

  ephone 13
   button 1:23

  ephone 14
       button 1:33
```

Where to Go Next

Softkey Display

The display of soft keys during different call states is managed using ephone templates. For more information, see Customize Softkeys, on page 925.

Feature Information for Creating Templates

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

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

Table 110: Feature Information for Templates

Feature Name	Cisco Unified CME Version	Feature Information
Ephone Templates	4.0	• The number of ephone templates that can be created was increased from 5 to 20. • More commands can be included in ephone templates.
	3.2	Ephone templates were introduced to manage soft keys. The only commands that can be used in ephone templates are the **softkeys** commands.
Ephone-dn Templates	4.0	Ephone-dn templates were introduced.
Phone Templates for SIP Phones	4.1	The maximum number of templates that can be configured was increased from 5 to 10.
	3.4	Voice-register templates were introduced for SIP Phones directly connected to a Cisco Unified CME router.

CHAPTER 48

Modify Cisco Unified IP Phone Options

This chapter describes the screen and button features available for Cisco Unified IP phones connected to Cisco Unified Communications Manager Express (Cisco Unified CME).

Information About Cisco Unified IP Phone Options

Clear Directory Entries

Cisco Unified CME 8.6 allows you to clear the display of call-history details such as missed, placed, and received call entries on your Cisco Unified SCCP IP phone's display screen. You can press the directory services button on most of the Cisco Unified IP phones or program a line button on 7931 phone to delete the display of phone number entries in the missed, placed, and received calls. The clear call directory feature is supported on Cisco Unified IP phones, 7960, 7961, 7970. 7971 and 8961.

To enable the clear directory entries feature, a call-history option is added to the **exclude** command. For more information on configuring phones to clear call-history details, see Clear Call-History Details from a SCCP Phone, on page 1449.

Enable Customized Background Images for Cisco Unified IP Phone 7970

The Cisco Unified IP Phone 7970 and 7971 support customized background images on the phone screen. To enable your Cisco Unified IP Phone 7970 or 7971 to display a customized background image, follow the procedure in the technical note at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_tech_note09186a008062495a.shtml.

Sample background images are available in the 7970-backgrounds.tar file at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Customized Button Layout

Cisco Unified CME 8.5 and later versions allow you to customize the display order of various button types on a phone using the button layout feature. The button layout feature allows you to customize the display of the following button types:

- Line buttons
- Speed Dial buttons
- BLF Speed Dial buttons
- Feature Buttons
- ServiceURL buttons

Cisco Unified CME 8.5 uses the **button layout** command is to populate buttons in any desired order. All buttons displayed on the phone follow the button-layout configuration. In the **button layout** command, the physical button number on the phone is specified under the *button-string* parameter of the **button layout** command. Buttons that are not defined under the button layout configuration are displayed as blank lines. Before configuring button layout on phones, line buttons, feature buttons (including privacy button), and url buttons must be configured through **line button**, **feature button** and **url button** commands, respectively.

Line Buttons

The button layout control feature allows you to populate buttons with corresponding physical line numbers or line number ranges. Line buttons that are not associated with a physical line are not displayed on the phone.You can customize any Cisco Unified SCCP IP phone button to function as a line button using the button command and specifying the position, button type, and directory number of the phone. For more information, see Configure Button Layout on SCCP Phones, on page 1454.

For Cisco Unified SIP phones, the first physical button must be a line button with a valid directory number. You can customize the other buttons using the **button** command and specifying the relative position (position index), button type, and directory number of the button. For more information, see Configure Button Layout on SIP Phones, on page 1456.

Speed Dial Buttons

You can customize the display of Speed Dial buttons to appear before, after, or between line buttons using the **speed-dial** command and specifying the position of the button. The button layout feature allows you to populate the buttons with corresponding physical line numbers or line number ranges. Buttons that do not have a physical line associated with them are not displayed on the phone.

BLF Speed Dial Buttons

The button layout feature allows you to display the BLF Speed-Dial buttons before, after or between the line buttons using the **blf-speed-dial** command with a specific position. Once the BLF speed-dial button is configured, the system populates the button with corresponding physical line number or range of line numbers. Buttons without a physical line association are not displayed on the phone.

Feature Buttons

Currently, privacy button is the only button available and is presented at the end of all the above mentioned buttons. With PLK feature you can enable most phone features on phone's physical buttons (line keys). This button layout feature requests all presented buttons to be configured via **button**, **speed-dial**, **blf-speed-dial**, **feature-button**, or **url-button** commands. The privacy-button is overridden by feature-button if there is one. For more information on configuring feature buttons on a line key, see Configure Feature Button on a Cisco

Unified SCCP Line Key, on page 1464 and Configure Feature Button on a Cisco Unified SIP Phone Line Key, on page 1462.

Note If the button-layout feature is configured in both ephone-template and logout profile (extension mobility) mode, configuration in the latter takes precedence. Button-layout configuration under ephone mode takes precedence in phones that do not have extension mobility (EM).

Note Privacy button is counted as a feature button on phones that support privacy button and do not have any feature button configured through the **feature-button** command.

URL Buttons

The button layout feature allows you to display the url button before, after, or even between the line buttons, speed dial buttons, BLF speed dial buttons, or feature buttons. For more information on configuring the URL button on a line key, see Configure Service URL Button on a SCCP Phone Line Key, on page 1460 and Configure Service URL Button on a SIP IP Phone Line Key, on page 1459.

Customized Phone User Interface Services

In Cisco Unified CME 8.5 and later, you can customize the availability of individual service items such as Extension Mobility, My Phone Apps, and Single Number Reach (SNR) on a phone's user interface by assigning individual service item to a button using the Programmable Line Key (PLK) url-button configuration. For more information, see Configure Service URL Button on a SCCP Phone Line Key, on page 1460.

You can limit the availability of an individual service item on a phone's user interface by disabling the configuration for services such as EM, My Phone Apps, and Local Directory and exclude the display of these services from the phone's user interface. You can use the exclude command under ephone-template mode to exclude the display of Extension Mobility (EM), My Phone Apps, and Local Directory. For more information, see Block Local Services on Phone User Interface, on page 1466.

If a directory service is enabled through PLK configuration, the PLK configuration takes precedence over the exclusion of directory services under ephone or ephone template configuration modes. The service is available through the button directly regardless of the exclusion of services configured under ephone and ephone-template modes.

In Cisco Unified CME 8.5 and later versions, you use the **exclude** command in ephone or ephone-template configuration mode to exclude the availability of local services such as EM, My Phone Apps, and Local Directory from a Cisco Unified SCCP IP phone's user interface.

In Cisco Unified CME 9.0 and later versions, you use the **exclude** command in voice register pool or voice register template configuration mode to exclude any of these local services from a Cisco Unified SIP IP phone's user interface.

Note Before Cisco Unified CME 9.0, you must configure the Local Directory service with the internal URL address.

In Cisco Unified CME 9.0 and later versions, the internal URL address is the default when no external URL address is configured.

Fixed Line-Feature Buttons for Cisco Unified IP Phone 7931G

In Cisco Unified CME 4.0(2) and later versions, you can select from two fixed button-layout formats to assign functionality to certain line buttons on a Cisco Unified IP Phone 7931G to support key system phone behavior. If you do not select a button set, no fixed set of feature/line buttons are defined.

The line button layout for the Cisco Unified IP Phone 7931G is a bottom-up array. Button 1 is at the bottom right of the array and button 24 is at the top left of the array.

Button set 1 includes two predefined feature buttons: button 24 is Menu and button 23 is Headset.

Button set 2 includes four predefined feature buttons: button 24 is Menu; button 23 is Headset; button 22 is Directories; and button 21 is Messages.

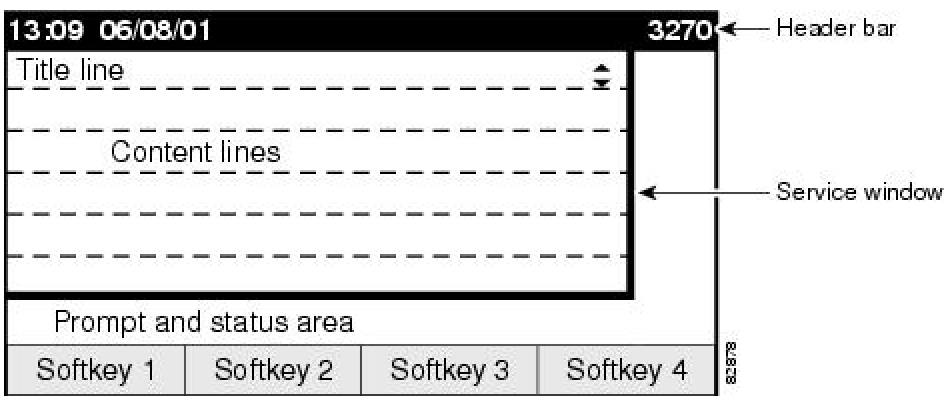
For configuration, see Select Button Layout for a Cisco Unified SCCP IP Phone 7931G, on page 1453.

Header Bar Display

You can customize the content of an IP phone header bar, which is the top line of the IP phone display.

The IP phone header bar, or top line, of a Cisco Unified IP Phone normally replicates the text that appears next to the first line button. The header bar is shown in Figure 69: Cisco Unified IP Phone Display, on page 1440. The header bar can, however, contain a user-definable message instead of the extension number. For example, the header bar can be used to display a name or the full E.164 number of the phone. If no description is specified, the header bar replicates the extension number that appears next to the first button on the phone.

Figure 69: Cisco Unified IP Phone Display



Phone Labels

Phone labels are configurable text strings that can be displayed instead of extension numbers next to line buttons on a Cisco Unified IP phone. By default, the number that is associated to a directory number, and assigned to a phone, is displayed next to the applicable button. The label feature allows you to enter a meaningful text string for each directory number so that a phone user with multiple lines can select a line by label instead of by phone number, thus eliminating the need to consult in-house phone directories. For configuration information, see Create Labels for Directory Numbers on SCCP Phones, on page 1471 or Create Labels for Directory Numbers on a SIP Phone, on page 1472.

Programmable Vendor Parameters for Phones

The vendorConfig section of the configuration file contains phone and display parameters that are read and implemented by a phone's firmware when that phone is booted. Only the parameters supported by the currently loaded firmware are available. The number and type of parameters may vary from one firmware version to the next.

The IP phone that downloads the configuration file will implement only those parameters that it can support and ignore configured parameters that it cannot implement. For example, a Cisco Unified IP Phone 7970G does not have a backlit display and cannot implement Backlight parameters regardless of whether they are configured. The following text shows the format of an entry in the configuration file:

```
<vendorConfig>
<parameter-name>parameter-value</parameter-name>
</vendorConfig>
```

For configuration information at the system level, see Modify Vendor Parameters for All SCCP Phones, on page 1479.

For configuration information for individual phones, see Modify Vendor Parameters for a Specific SCCP Phone, on page 1481.

Push-to-Talk

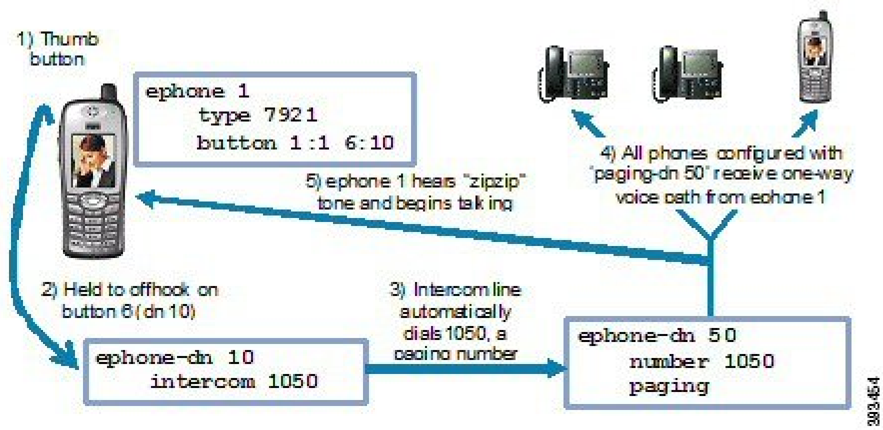
This feature allows one-way Push-to-Talk (PTT) in Cisco Unified CME 7.0 and later versions without requiring an external server to support the functionality. PTT is supported in firmware version 1.0.4 and later versions on Cisco Unified Wireless IP Phone 7921 and 7925 with a thumb button.

In the following figure, button1/DN 1 is configured as the primary line for this phone. Button 6/ DN 10 is configured for PTT and is the line that is triggered by pushing the thumb button on this phone.

- Holding down on the thumb button causes the configured DN on the phone to go off-hook.
- The thumb button utilizes an intercom DN that targets a paging number (1050).
- The targeted paging group (DN 50) can be unicast or multicast or both.
- Users will hear a “zipzip” tone when call path is set up.
- All other keys on the phone are locked during this operation.

- Releasing the thumb button ends the call.

Figure 70: PTT Call Flow



For configuration information, see Configure One-Way Push-to-Talk on Cisco Unified SCCP Wireless IP Phones, on page 1483.

Support for Cisco Jabber

Cisco Unified CME 8.6 and later versions support Cisco Jabber. The softphone SIP client is an iPhone application and works as a SIP softphone. The SIP softphone client is capable of supporting VoIP over WLAN. Cisco Unified CME 8.6 supports supplementary services such as Hold, Resume, Transfer, Call Park, and Call Pickup for the softphone SIP client.

To configure visual voicemail settings on Cisco Jabber, the ability to edit user settings should be enabled, see Enable Edit User Settings, on page 1446.

You can configure the softphone SIP client using the phone type **CiscoJabber-iOS** option. For more information on configuring Cisco Jabber, see Configure Cisco Jabber, on page 1447.

Restriction Hand-off call to GSM is not supported.

Cisco Jabber for iPhone is only supported with iOS 5.

Call Park and Pickup

In Cisco SIP client, when you press the Home action button, the call continues and the application runs in the background.

When a call is parked and the Cisco iPhone SIP client unregisters because of a power outage, out of range access point, or simply because you pressed the Home action button, the SIP client displays a pop-up with an option to pickup the call (the parked call). This only happens when the client re-registers (before the configured park timer expires or call gets dropped).

Dial Rules

Cisco softphone SIP client uses the dial rules to integrate with the Lightweight Directory Access Protocol (LDAP) directory server. The Cisco softphone SIP client also uses dial rules such as application dial rule and directory lookup rule to translate the outgoing phone numbers and display the incoming phone numbers with a rich caller ID. A rich caller ID displays a caller's name, caller's picture, or caller's phone number, or the information saved in the phone's directory.

You can create the application dial rule or directory lookup rule xml files and add these files to a tftp server. The Cisco softphone SIP client can download the dial rules using the **url** [**ldapserver** *string*], **url** [**AppDialRule** *string*] **url** [**DirLookupRule** *string*] command under voice register template configuration mode. You must apply the voice registration configuration to the voice register pool configuration mode. For more information, see Configure Dial Rules for Cisco Softphone SIP Client, on page 1451.

Cisco Jabber Client Support on CME

Cisco Jabber Client is a SIP-based soft client with integrated Instant Messaging and presence functionality, and uses the new Client Services Framework 2nd Generation (CSF2G) architecture.

CSF is a unified communications engine that is reused by multiple Cisco PC-based clients and mobile clients. The client is identified by a device ID name that can be configured under the voice register pool in Cisco Unified CME. You should configure the username and password under voice register pool to identify the user logging into Cisco Unified CME through Cisco Jabber client. The device discovery process uses HTTPS connection. Therefore, you should configure the secure HTTP on Cisco Unified CME.

A new phone type, 'Jabber-CSF-Client' has been added to configure the Cisco Jabber client under voice register pool. This can be used to configure any CSF based Cisco Jabber client. In CME-10.0 we used the type 'Jabber-Win' to configure Cisco Jabber client. In CME-10.5 this type is deprecated and the new 'Jabber-CSF-Client' should be used to configure Cisco Jabber client as well.

Cisco Jabber CSF client can be provisioned in 2 modes: Full UC mode (with integrated IM and Presence services) and Phone only mode. From CME-10.5 onwards the phone-only mode of Cisco Jabber CSF devices is also supported. This can be configured with the option 'phone-mode phone-only' under 'voice register global' or 'voice register pool' or 'voice register template' config.

If the Jabber client is installed in phone only mode then no extra configuration is required on CME. The normal Jabber configuration should be sufficient. For more information on installing Jabber client in phone mode refer to following guide- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/9_2/JABW_BK_C9731738_00_jabber-windows-install-config.html

If the Jabber client is installed in Full UC mode and you want to enable the phone only mode from CME, then the 'phone-mode' configuration is required as mentioned in the configuration section.

Table 111: Cisco Jabber Client Support Versions, on page 1443 lists the Cisco Jabber Client Support versions along with the corresponding CME and Jabber client versions:

Table 111: Cisco Jabber Client Support Versions

Cisco CSF Device Type	Unified CME Supported Version	Jabber Client Version	
Cisco Jabber for MAC and Windows (phone-only)	10.0	9.1.0	
	10.5	9.2.1	

Restrictions

- The Cisco Jabber CSF client (full UC mode) on Unified Communications Manager Express should register with a presence server such as cloud-based WebEx server, to enable the telephony features on Jabber client.
- The Cisco Jabber CSF client supports only the visual voice mail functionality using Internet Message Access Protocol (IMAP) on the Cisco Unity Connection.
- The Cisco Jabber CSF client supports only the softphone mode with Cisco Unified CME.
- Desk phone mode is not supported.
- The following Cisco Jabber CSF type of devices are not supported:
  - Cisco Jabber for MAC (phone-only mode)
  - Cisco Jabber for iPhone (both full UC mode and phone-only mode)
  - Cisco Jabber for Android (both full UC mode and phone-only mode)
  - Cisco Jabber for iPad (both full UC mode and phone-only mode)

For configuration information, see Configure Cisco Jabber for CSF Client in Cisco Unified CME, on page 1485.

For configuration examples, see Example for Configuring Cisco Jabber CSF Client, on page 1488.

System Message Display

The System Message Display feature allows you to specify a custom text or display message to appear in the lower part of the display window on display-capable IP phones. If you do not set a custom text or display message, the default message “Cisco Unified CME” is displayed.

When you specify a text message, the number of characters that can be displayed is not fixed because IP phones typically use a proportional (as opposed to fixed-width) font. There is room for approximately 30 alphanumeric characters.

The display message is refreshed with a new message after one of the following events occurs:

- Busy phone goes back on-hook.
- idle phone receives a keepalive message.
- Phone is restarted.

The file-display feature allows you to specify a file to display on display-capable IP phones when they are not in use. You can use this feature to provide the phone display with a system message that is refreshed at configurable intervals, similar to the way that the text message feature provides a message. The difference between the two is that the system text message feature displays a single line of text at the bottom of the phone display, whereas the system display message feature can use the entire display area and contain graphic images.

URL Provisioning for Feature Buttons

URL provisioning for programmable feature buttons allows you to specify alternative XML files to access using the feature buttons on IP phones.

Certain phones, such as the Cisco Unified IP Phone 7940, 7940G, 7960, and 7960G, have programmable feature buttons that invoke noncall-related services. The four buttons—Services, Directories, Messages, and Information (the i button)—are linked to appropriate feature operations through URLs. The fifth button—Settings—is managed entirely by the phone.

The feature buttons are provisioned with specific URLs. The URLs link to XML web pages formatted with XML tags that the Cisco Unified IP phone understands and uses. When you press a feature button, the Cisco Unified IP phone uses the configured URL to access the appropriate XML web page for instructions. The web page sends instructions to the Cisco Unified IP phone to display information on the screen for users to navigate. Phone users can select options and enter information by using soft keys and the scroll button.

Operation of these feature buttons is determined by the capabilities of the Cisco Unified IP phone and the content of the specified URL.

In Cisco Unified CME 4.2 and later versions, up to eight URLs can be configured for the Services feature button by using an ephone template to apply the configuration to one or more supported SCCP phones. If you use an ephone template to configure services URLs for one or SCCP phones and you also configure a system-level services URL in telephony-service configuration mode, the value set in telephony-service configuration mode appears first in the list of services displayed when the phone user presses the Services feature button. Cisco Unified CME self-hosted services, such as Extension Mobility, always appears last in the list of options displayed for the Services feature button.

For configuration information, see Provision URLs for Feature Buttons for SCCP Phones, on page 1476.

My Phone Apps for Cisco Unified SIP IP Phones

Before Cisco Unified CME 9.0, the My Phone Apps features were only supported on Cisco Unified SCCP IP phones.

In Cisco Unified CME 9.0 and later versions, support is added for My Phone Apps feature on Cisco Unified SIP IP phones.

My Phone Apps is a user application that enables the following settings to be configured using the menu available with the phone's Services feature buttons:

- add, modify, or delete Speed Dial
- add, modify, or delete Fast Dial
- add, modify, or delete BLF Speed Dial
- change SNR DN
- perform after-hour login
- reset the phone

The My Phone Apps features are available on both Extension Mobility (EM) and non-EM phones. For EM phones, the user login service allows the user to temporarily access a physical phone other than their own and utilize their personal settings as if the phone is their own desk phone. Any change in settings follows the user to the next phone they access. For non-EM phones, any change in settings remains with the physical phone.

Configure Cisco Unified IP Phone Options

Enable Edit User Settings

Before You Begin

Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **service phone** *parameter-name parameter-value*
5. **voice register global**
6. **create profile**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**service phone** *parameter-name parameter-value* **Example:** `Router(config-telephony)# service phone paramEdibility 1`	Enables the edit user settings.
Step 5	**voice register global** **Example:** `Router(config-telephony)# voice register global`	Enters voice register global configuration mode.

	Command or Action	Purpose
Step 6	**create profile** **Example:** `Router(config-register-global)# create profile`	Generates provisioning files required for SIP phones and writes the file to the location specified with the **tftp-path** command.
Step 7	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure Cisco Jabber

Restriction

- Conferencing feature through the Add Call action key is not supported.
- Call hand off to the mobile network is not supported.
- Shared line is not supported.

Before You Begin

Cisco Unified CME 8.6 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool tag*
4. **id mac** *address*
5. **type** *phone-type*
6. **registration timer max** *seconds* **min** *seconds*
7. **number** *tag* **dn** *dn-tag*
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool** *pool tag* **Example:** `Router(config)#voice register pool 8`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 4	**id mac** *address* **Example:** `Router((config-register-pool)# id mac 9084.0D0B.DF81`	Explicitly identifies a locally available individual SIP phone to support a degree of authentication.
Step 5	**type** *phone-type* **Example:** `Router(config-register-pool)# type CiscoMobile-iOS`	Defines a phone type for the SIP phone being configured. After configuring the type, Cisco Unified CME automatically changes the SIP session transport to TCP. Also the registration timer default changes to 720 seconds. **Note** CiscoMobile client only supports SIP TCP transport and requires the re-registration timer to be greater than 660 seconds to support multitasking on Apple's operating system (iOS).
Step 6	**registration timer max** *seconds* **min** *seconds* **Example:** `Router(config-register-pool)registration-timer max 770 min 660`	(Optional) Allows to set the value for the expiration of keepalive registration-time (in seconds). • **max** *seconds*— Maximum registration time in seconds. Default is 720 seconds. • **min** *seconds*—Minimum registration time in seconds. Default is 660 seconds. **Note** You must configure a minimum timer value of 660 seconds to allow the CiscoMobile client application to work in the background.
Step 7	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 10`	Associates a directory number with the SIP phone being configured. • **dn** *dn-tag*—identifies the directory number for this SIP phone as defined by the voice register dn command.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Clear Call-History Details from a SCCP Phone

To clear the display of Call History details such as Missed Calls, Placed Calls, and Received Calls, from a SCCP IP phone user interface, follow these steps:

Before You Begin

To enable phones to send an HTTP GET request, url directories must be the default (not configured) or configured as `http://<CME's ip address>/localdirectory`.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
    - **ephone** *phone-tag*
    - **ephone template** *template tag*
4. **exclude** [**em** | **myphoneapp** | **directory** | **call-history**]
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	Enter one of the following commands: • **ephone** *phone-tag* • **ephone template** *template tag* **Example:** `Router(config)# ephone 10`	Enters ephone configuration mode. • *phone-tag*—Unique number of the phone for which you want to exclude local services such as Extension Mobility, My Phone Apps, and Local Directory.

	Command or Action	Purpose
Step 4	**exclude** [**em** | **myphoneapp** | **directory** | **call-history**] **Example:** `Router(config-ephone)#exclude call-history`	Excludes local services (EM, My Phone Apps, Local Directory, and Call History) from displaying on phone's user interface. • em—Excludes Extension Mobility (EM) from the phone's user interface. • myphoneapp —Excludes My Phone App service from the phone's user interface. • directory —Excludes Local Directory service from the phone's user interface. • call-history—Excludes entries from Call History on the phone's user interface.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

The following example shows call-history as excluded from ephone 10 and ephone-template 5:

```
!
telephony-service
 max-ephones 40
 max-dn 100
 max-conferences 8 gain -6
 transfer-system full-consult
!
!
ephone-template  5
 exclude call-history
!
!
ephone  10
 exclude call-history
 device-security-mode none
!
```

Troubleshooting Tips for Clearing Call-History Details from a SCCP Phone

The following is a list of troubleshooting tips for successful implementation of this feature:

- Make sure that the local directory XML tag is configured and provisioned correctly.
- Check the attribute for <directoryURL> tag in the xml file (it must be set up with http://<CME's ip address>/localdirectory) and the phone must be restarted with this XML cnf file.
- Make sure that the phone sends out an HTTP GET request.
- Make sure that the HTTP GET request in the Cisco Unified CME log with “deb ip http url” is enabled.
- Make sure that the Clear Directory Entries request is sent to the phone.

- Check the Missed Calls, Placed Calls, and Received Calls on your phone's local directory.

Configure Dial Rules for Cisco Softphone SIP Client

Before You Begin

Cisco Unified CME 8.6 or a later version.

Support for **idle** *url* is available only on Unified CME 12.0 and later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template tag*
4. **url** {**AppDialRule** *string* | **DirLookupRule** *string* | **ldapServer** *string* | **idle** *url* | **service** *url*}
5. **voice register pool** *pool tag*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register template** *template tag* **Example:** `Router(config)#voice register template 8`	Enters voice register template configuration mode to define a template of common parameters for SIP phones in Cisco Unified CME.

	Command or Action	Purpose

Step 4	**url** {**AppDialRule** *string* | **DirLookupRule** *string* | **ldapServer** *string* | **idle** *url* | **service** *url*}
	
	Example:
	`Router(config-register-temp)# url ldapServer ldap.abcd.com`
	`Router(config-register-temp)# url AppDialRule tftp://10.1.1.1/AppDialRules.xml`
	`Router(config-register-temp)# url DirLookupRule tftp://10.1.1.1/DirLookupRules.xml`
	`Router(config-register-temp)# url idle http://www.mycompany.com/files/logo.xml idle-timeout 12`
	`Router(config-register-temp)# url service http://10.0.0.4/CCMUser/123456/urltest.html`
		Allows to define SIP phone URLs to configure Application Dial Rule, Directory Lookup Dial Rule, LDAP server, idle url, and service url in voice register template configuration mode.
		• **ldapserver** *string* **—**LDAP server URL.
		• **AppDialRule** *string* **—**Application dial rule URL.
		• **DirLookupRule** *string***—**Directory lookup rule URL.
		• **idle** *url* **—**Defines the location of a file to display on phones that are not in use and specifies the interval between refreshes of the display, in seconds.
		• **service** *url* **—**Uses the information at the specified URL for invoking phone services.

Step 5	**voice register pool** *pool tag* **Example:** `Router(config)#voice register pool 8`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 6	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows dial rules configured under voice register template 2:

```
!
voice register template 2
 url ldapServer ldap.abcd.com
 url AppDialRule tftp://10.1.1.1/AppDialRules.xml
 url DirLookupRule tftp://10.1.1.1/DirLookupRules.xml
!
```

The following is a sample of Application Dial Rule content:

```
Router#more flash:AppDialRules.xml
<?xml version="1.0" encoding="UTF-8"?><DialRules>
        <DialRule BeginsWith="+1" NumDigits="12" DigitsToRemove="1" PrefixWith="9"/>
        <DialRule BeginsWith="+1" NumDigits="12" DigitsToRemove="1" PrefixWith="9"/>
        <DialRule BeginsWith="919" NumDigits="10" DigitsToRemove="3" PrefixWith="9"/>
        <DialRule BeginsWith="1" NumDigits="11" DigitsToRemove="0" PrefixWith="9"/>
        <DialRule BeginsWith="" NumDigits="10" DigitsToRemove="0" PrefixWith="91"/>
        <DialRule BeginsWith="" NumDigits="7" DigitsToRemove="0" PrefixWith="9"/>
        <DialRule BeginsWith="+" NumDigits="13" DigitsToRemove="1" PrefixWith="9011"/>
        <DialRule BeginsWith="+" NumDigits="14" DigitsToRemove="1" PrefixWith="9011"/>
        <DialRule BeginsWith="+" NumDigits="15" DigitsToRemove="1" PrefixWith="9011"/>

        <DialRule BeginsWith="+" NumDigits="12" DigitsToRemove="1" PrefixWith="9011"/>
        <DialRule BeginsWith="+" NumDigits="11" DigitsToRemove="1" PrefixWith="9011"/>
</DialRules>
```

Select Button Layout for a Cisco Unified SCCP IP Phone 7931G

Before You Begin

Cisco Unified CME 4.0(2) or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **button-layout** *phone-type* {**1** | **2**}
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone-template** *template-tag* **Example:** `Router(config)# ephone-template 15`	Enters ephone-template configuration mode to create an ephone template.
Step 4	**button-layout** *phone-type* {**1** | **2**} **Example:** `Router(config-ephone-template)# button-layout 7931 2`	Specifies which fixed set of feature buttons appears on a Cisco Unified IP Phone 7931G that uses a template in which this is configured. • **1**—Includes two predefined feature buttons: button 24 is Menu and button 23 is Headset. • **2**—Includes four predefined feature buttons: button 24 is Menu; button 23 is Headset; button 22 is Directories; and button 21 is Messages.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits from this command mode to the next highest mode in the configuration mode hierarchy.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 15`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Configure Button Layout on SCCP Phones

Before You Begin

- Cisco Unified CME 8.5 or later versions.
- Button types such as, line, feature, url, speed-dial, and blf-speed-dial are configured using commands such as, **button**, **feature-button** or **privacy-button**, **url-button**, **speed-dial**, and **blf-speed-dial** respectively.
- First button must be configured as line button.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template tag*
4. **button-layout** [*button-string* | *button-type*]
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone-template** *template tag* **Example:** `Router(config)# ephone 10`	Enters ephone template configuration mode to create an ephone template.

Step 4	**button-layout** [*button-string* | *button-type*]
	
	Example:
	`Router(config-ephone-template)#button-layout 1 line`
	`Router(config-ephone-template)#button-layout 2,5 speed-dial`
	`Router(config-ephone-template)#button-layout 3,6 blfspeed-dial`
	`Router(config-ephone-template)#button-layout 4,7,9 feature`
	`Router(config-ephone-template)# button-layout 8,11 url`
		Assigns physical button numbers or ranges of numbers with button types.
		
		• *button-string*—Specifies a coma separated list of physical button number or ranges of button numbers.
		
		• *button-type*—Specifies one of the following button types: Line, Speed-Dial, BLF-Speed-Dial, Feature, URL. Button number specifies the relative display order of the button within the button type (line button, speed-dial, blf-speed-dial, feature-button or url-button).
		
		Note To facilitate phone provisioning, the first line button should always be a line button.
		Note When no feature-buttons are configured, privacy button is counted as a feature button.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits from this command mode to the next highest mode in the configuration mode hierarchy.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 10`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Exits configuration mode and enters privileged EXEC mode.

Examples

```
Router# show telephony-service ephone-template
ephone-template  10
 button-layout 1 line
 button-layout 2,5 speed-dial
 button-layout 3,6 blf-speed-dial
 button-layout 4,7,9 feature
 button-layout 8,11 url
```

What to Do Next

If you are done modifying parameters for SCCP phones in Cisco Unified CME, restart the phones.

Configure Button Layout on SIP Phones

Note You can not change the button number in the line button or index command through button layout configuration because the button number specifies the relative display order of the button within the button type (line button, speed-dial, blf-speed-dial, feature button, or url button).

Before You Begin

- Cisco Unified CME 8.5 or later versions.
- Button types (line button, feature button, url-button, speed dial button, and blf speed dial button) must be configured before configuring button layout.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **button-layout** [*button-string*] [*button-type*]
5. **exit**
6. **voice register pool** *pool-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters voice register template configuration mode to create a SIP phone template. • template-tag—Range: 1 to 10.

Step 4	**button-layout** [*button-string*] [*button-type*]
	
	Example:
	`Router(config-register-template)#button-layout 1 line`
	`Router(config-register-template)#button-layout 2, 5 speed-dial`
	`Router(config-register-template)#button-layout 3, 6 blfspeed-dial`
	`Router(config-register-template)#button-layout 4,7,9 feature-button`
	`Router(config-register-template)# button-layout 8,11 url-button`
		Assigns physical button numbers or ranges of numbers with button types.
		• *button-string*—Specifies a coma separated list of physical button number or ranges of button numbers.
		• *button-type*—Specifies one of the following button types: Line, Speed-Dial, BLF-Speed-Dial, Feature, URL.
		Note To facilitate phone provisioning, the first line button should always be a line button.
		Note Privacy-button is counted as a feature-button in this configuration if no feature-button is configured.

Step 5	**exit** **Example:** `Router(config-register-template)# exit`	Exits voice register template configuration mode.

	Command or Action	Purpose
Step 6	**voice register pool** *pool-tag* **Example:** `Router(config)# voice register pool 10`	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies a SIP phone template to the phone you are configuring. • *template-tag*— Template tag that was created with the voice register template command in Step 3, on page 1457.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.

Examples

```
Router# show voice register template all
!
voice register dn  65
 number 3065
 name SIP-7965
 label SIP3065
!
voice register template  5
 button-layout 1 line
 button-layout 2,5 speed-dial
 button-layout 3,6 blf-speed-dial
 button-layout 4,7,9 feature-button
 button-layout 8,11 url-button
!
voice register template  2
 button-layout 1,5 line<
 button-layout 4 speed-dial
 button-layout 3,6 blf-speed-dial
 button-layout 7,9 feature-button
 button-layout 8,10-11 url-button
!
```

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Configure Service URL Button on a SIP IP Phone Line Key

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **url-button** [**index** *number*] [**url** *location]* [**url** *name*]
5. **exit**
6. **voice register pool** *phone-tag*
7. **template** *template-tag*
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 register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.
Step 4	**url-button** [**index** *number*] [**url** *location]* [**url** *name*] **Example:** `Router(config-register-temp)url-button 1 http:// www.cisco.com`	Configures a service url feature button on a line key. • Index number—Unique index number. Range: 1 to 8. • url *location*—Location of the url. • url *name*—Service url with maximum length of 31 characters.
Step 5	**exit** **Example:** `Router(config-register-temp)# exit`	Exits ephone-template configuration mode.
Step 6	**voice register pool** *phone-tag*	Enters ephone configuration mode.

	Command or Action	Purpose
	Example: `Router(config)# voice register pool 12`	• *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3, on page 1459.
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows url buttons configured in voice register template 1:

```
Router# show run
!
voice register template  1

url-button 1 http://9.10.10.254:80/localdirectory/query My_Dir
url-button 5 http://www.yahoo.com Yahoo

!
voice register pool  50
!
```

What to Do Next

If you are done configuring the url buttons for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Configure Service URL Button on a SCCP Phone Line Key

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone template** *template-tag*
4. **url-button** *index* **type** | *url* [*name*]
5. **exit**
6. **ephone** phone-tag
7. **ephone-template** *template-tag*
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	**ephone template** *template-tag* **Example:** `Router(config)# ephone template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.

Step 4	**url-button** *index* **type** | *url* [*name*]
	
	Example:
	
	`Router#(config-ephone-template)#url-button 1 myphoneapp`
	
	`Router(config-ephone-template)#url-button 2 em`
	
	`Router(config-ephone-template)#url-button 3 snr`
	`Router (config-ephone-template)#url-button 4 http://www.cisco.com`
		Configures a service url feature button on a line key.
		• *Index*—Unique index number. Range: 1 to 8.
		• **type**—Type of service url button. Following types of url service buttons are available:
		  • myphoneapp: My phone application configured under phone user interface.
		  • em: Extension Mobility
		  • snr: Single Number Reach
		• *url name*—Service url with maximum length of 31 characters.

Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** phone-tag **Example:** `Router(config)#ephone 36`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 5`	Applies an ephone template to the ephone that is being configured.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Examples

The following example shows three url buttons configured for line keys:

```
!
!
!
ephone-template  5
 url-button 1 em
 url-button 2 mphoneapp mphoneapp
 url-button 3 snr
!
ephone  36
 ephone-template 5
```

What to Do Next

If you are done configuring the url buttons for phones in Cisco Unified CME, restart the phones.

Configure Feature Button on a Cisco Unified SIP Phone Line Key

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **feature-button** [*index*] [*feature identifier*]
5. **exit**
6. **voice register pool** *phone-tag*
7. **template** *template-tag*
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register template** *template-tag* **Example:** `Router(config)# voice register template 5`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10. **Note** Feature button can be configured under **voice register pool** or **voice register template** configuration mode. If both configurations are applied to the **voice register pool**, the feature button configuration under **voice register pool** takes precedence.

Step 4	**feature-button** [*index*] [*feature identifier*]
	
	Example:
	`Router(config-voice-register-template)feature-button 1 DnD`
	`Router(config-voice-register-template)feature-button 2 EndCall`
	`Router(config-voice-register-template)feature-button 3 Cfwdall`
		Configures a feature button on line key.
		• *index*—One of the 12 index numbers for a specific feature type.
		• *feature identifier*—Unique identifier for a feature. One of the following feature or stimulus IDs: Redial, Hold, Trnsfer, Cfwdall, Privacy, MeetMe, Confrn, Park, Pickup, Gpickup, Mobility, NewCall, EndCall, Dnd, ConfList, NewCall, HLog, Trnsfer.

Step 5	**exit** **Example:** `Router(config-register-temp)# exit`	Exits ephone-template configuration mode.
Step 6	**voice register pool** *phone-tag* **Example:** `Router(config)# voice register pool 12`	Enters ephone configuration mode. • *phone-tag*—Unique number that identifies this ephone during configuration tasks.
Step 7	**template** *template-tag* **Example:** `Router(config-register-pool)# template 5`	Applies the ephone template to the phone. • *template-tag*—Unique identifier of the template that you created in Step 3, on page 1463
Step 8	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows three feature buttons configured for line keys:

```
voice register template  5
 feature-button 1 DnD
 feature-button 2 EndCall
 feature-button 3 Cfwdall
!
    !
voice register pool 12
template 5
```

What to Do Next

If you are done configuring the url buttons for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Configure Feature Button on a Cisco Unified SCCP Line Key

Note

- Answer, Select, cBarge, Join, and Resume features are not supported as PLKs.
- Feature buttons are only supported on Cisco Unified IP Phones 6911, 7941, 7942, 7945, 7961, 7962, 7965. 7970, 7971, and 7975 with SCCP v12 or later versions.
- Any features available through hard button are not be provisioned. Use the show ephone register detail command to verify why the features buttons are not provisioned.
- Not all feature buttons are supported on Cisco Unified IP Phone 6911 phone. Call Forward, Pickup, Group Pickup, and MeetMe are the only feature buttons supported on the Cisco Unified IP Phone 6911.
- The privacy-button is available on Cisco Unified IP phones running a SCCP v8 or later. Privacy-buttton is overridden by any other feature-button available.
- Locales are not supported on Cisco Unified IP Phone 7914.
- Locales are not supported for Cancel Call Waiting or Live Recording feature-buttons.
- The feature state for DnD, Hlog, Privacy, Login, and Night Service feature-buttons are indicated by an LED.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone template** *template-tag*
4. **feature-button** *index feature identifier*
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone template** *template-tag* **Example:** `Router(config)# ephone template 10`	Enters ephone-template configuration mode to create an ephone template. • *template-tag*—Unique identifier for the ephone template that is being created. Range: 1 to 10.
Step 4	**feature-button** *index feature identifier* **Example:** `Router(config-ephone-template)feature-button 1 hold`	Configures a feature button on line key • *index*—index number, one from 25 for a specific feature type. • *feature identifier*—feature ID or stimulus ID.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 5`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.

	Command or Action	Purpose
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 10`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Examples

The following example shows feature buttons configured for line keys:

```
!
!
!
ephone-template  10
 feature-button 1 Park
 feature-button 2 MeetMe
 feature-button 3 CallBack
!
!
ephone-template 10
```

What to Do Next

If you are done configuring the feature buttons for phones in Cisco Unified CME, restart the phones.

Block Local Services on Phone User Interface

To block the display and availability of local services such as Local Directory, Extension Mobility (EM), and My Phone Apps on a SCCP IP phone's user interface, perform the following steps.

Before You Begin

Cisco Unified CME 8.5 or later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag* or **ephone template** *template tag*
4. **exclude** [**em** | **myphoneapp** | **directory**]
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** *phone-tag* or **ephone template** *template tag* **Example:** `Router(config)# ephone 10`	Enters ephone configuration mode. • *phone-tag*—Unique number of the phone for which you want to exclude local services such as Extension Mobility, My Phone Apps, and Local Directory.
Step 4	**exclude** [**em** | **myphoneapp** | **directory**] **Example:** `Router(config-ephone)#exclude directory em`	Excludes local services (EM, My Phone Apps, and Local Directory) from displaying on phone's user interface. • em—Excludes Extension Mobility (EM) from the phone's user interface. • myphoneapp —Excludes My Phone App service from the phone's user interface. • directory —Excludes Local Directory service from the phone's user interface.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Examples

The following example shows the Local Directory and Extension Mobility services excluded from the phone user interface:

```
ephone  10
 exclude directory em
 device-security-mode none
 description sccp7961
 mac-address 0007.0E57.7561
```

Modify Header Bar Display on SCCP Phones

Before You Begin

Directory number to be modified is already configured. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **description** *display-text*
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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 55`	Enters ephone-dn configuration mode.
Step 4	**description** *display-text* **Example:** `Router(config-ephone-dn)# description 408-555-0134`	Defines a description for the header bar of a display-capable IP phone on which this ephone-dn appears as the first line. • *display-text*—Alphanumeric character string, up to 40 characters. String is truncated to 14 characters in the display.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Modify Header Bar Display Supported SIP Phones

Restriction This feature is supported only on Cisco Unified IP Phone 7940, 7940G, 7960, and 7960G.

Before You Begin

Cisco CME 3.4 or a a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **description** *string*
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 register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone in Cisco Unified CME.
Step 4	**description** *string* **Example:** `Router(config-register-pool)# description 408-555-0100`	Defines a customized description that appears in the header bar of supported Cisco Unified IP phones • Truncated to 14 characters in the display. • If string contains spaces, enclose the string in quotation marks.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Verify Header Bar Display

Use the **show running-config** command to verify your configuration. Descriptions for directory numbers are listed in the ephone-dn and voice-register dn portions of the output.

Example:

```
Router# show running-config

    ephone-dn  1  dual-line
     number 150 secondary 151
     description 555-0150
     call-forward busy 160
     call-forward noan 160 timeout 10
     huntstop channel
     no huntstop
    !
    !
    !
    voice-register dn 1
     number 1101
     description 555-0101
```

Troubleshooting Header Bar Display

show telephony-service ephone

Use this command to ensure that the ephone-dn to which you applied the description appears on the first button on the ephone. In the example below, ephone-dn 22 has the description in the phone display header bar.

```
Router# show telephony-service ephone

    ephone-dn 22
```

```
 number 2149
 description 408-555-0149

ephone 34
 mac-address 0030.94C3.F96A
 button  1:22 2:23 3:24
 speed-dial 1 5004
 speed-dial 2 5001
```

Create Labels for Directory Numbers on SCCP Phones

To create a label to display in place of the number next to a line button, perform the following steps.

Before You Begin

Directory number for which the label is to be created is already configured. For configuration information, see Create Directory Numbers for SCCP Phones, on page 253.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **label** *label-string*
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-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 1`	Enters ephone-dn configuration mode. • *dn-tag*—Unique sequence number that identifies the ephone-dn to which the label is to be associated.

	Command or Action	Purpose
Step 4	**label** *label-string* **Example:** `Router(config-ephone-dn)# label user1`	Creates a custom label that is displayed on the phone next to the line button that is associated with this ephone-dn. The custom label replaces the default label, which is the number that was assigned to this ephone-dn. • *label-string*—String of up to 30 alphanumeric characters that provides the label text.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Create Labels for Directory Numbers on a SIP Phone

To create label to be displayed in place of a directory number for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI), perform the following steps for each label to be created.

Restriction Only one label is permitted per directory number.

Before You Begin

- Cisco CME 3.4 or a later version.
- Directory number for which the label is to be created is already configured and must already have a number assigned by using the **number (voice register dn)** command. For configuration information, see Create Directory Numbers for SIP Phones, on page 263.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **label** *string*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register dn** *dn-tag* **Example:** `Router(config-register-global)# voice register dn 17`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI).
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 7001`	Defines a valid number for a directory number.
Step 5	**label** *string* **Example:** `Router(config-register-dn)# label user01`	Creates a text identifier, instead of a phone-number display, for a directory number that appears on a SIP phone console.
Step 6	**end** **Example:** `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Verify Labels

Use the **show running-config** command to verify your configuration. Descriptions for directory numbers are listed in the ephone-dn and voice-register dn portions of the output.

`Router#` **show running-config**

```
ephone-dn  1  dual-line
 number 150 secondary 151
 label MyLine
 call-forward busy 160
 call-forward noan 160 timeout 10
 huntstop channel
 no huntstop
!
!
!
voice-register dn 1
 number 1101
 label MyLine
```

Modify System Message Display on SCCP Phone Screen

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **system message** *text-message*
5. **url idle** *url* **idle-timeout** *seconds*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**system message** *text-message*	Defines a text message to display when a phone is idle.

	Command or Action	Purpose
	Example: `Router(config-telephony)# system message ABC Company`	• *text-message*—Alphanumeric string to display. Display uses proportional-width font, so the number of characters that are displayed varies based on the width of the characters that are used. The maximum number of displayed characters is approximately 30.
Step 5	**url idle** *url* **idle-timeout** *seconds* **Example:** `Router(config-telephony)# url idle http://www.abcwrecking.com/public/logo idle-timeout 35`	Defines the location of a file to display on phones that are not in use and specifies the interval between refreshes of the display, in seconds. • *url*—Any URL that conforms to RFC 2396. • *seconds*—Time interval between display refreshes, in seconds. Range is 0 to 300.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

What to Do Next

After configuring the url idle command, you must reset phones. See Use the reset Command on SCCP Phones, on page 399.

Verify System Message Display

Use the **show running-config** command to verify your configuration. System message display is listed in the telephony-service portion of the output.

```
Router# show running-config

telephony-service
 fxo hook-flash
 load 7960-7940 P00307020300
 load 7914 S00104000100
 max-ephones 100
 max-dn 500
 ip source-address 10.153.13.121 port 2000
 max-redirect 20
 timeouts ringing 100
 system message XYZ Company
 voicemail 7189
 max-conferences 8 gain -6
 call-forward pattern .T
```

```
moh flash:music-on-hold.au
multicast moh 239.10.10.1 port 2000
web admin system name server1 password server1
dn-webedit
time-webedit
transfer-system full-consult
transfer-pattern 92......
transfer-pattern 91..........
transfer-pattern 93......
transfer-pattern 94......
transfer-pattern 95......
transfer-pattern 96......
transfer-pattern 97......
transfer-pattern 98......
transfer-pattern 99......
transfer-pattern .T
secondary-dialtone 9
create cnf-files version-stamp Jan 01 2002 00:00:00
```

Troubleshooting System Message Display

Ensure that the HTTP server is enabled.

Provision URLs for Feature Buttons for SCCP Phones

To customize URLs for feature buttons in the Sep*.conf.xml configuration file for SCCP phones, perform the following steps.

Restriction

- Operation of these services is determined by the Cisco Unified IP phone capabilities and the content of the specified URL.
- Provisioning a URL to access help screens using the i or ? buttons on a phone is not supported.
- Provisioning the directory URL to select an external directory resource disables the Cisco Unified CME local directory service.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **url** {**directories** | **information** | **messages** | **services**} *url*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**url** {**directories** | **information** | **messages** | **services**} *url* **Example:** `Router(config-telephony)# url directories http://10.4.212.4/localdirectory`	Provisions URLs for the four programmable feature buttons (Directories, Information, Messages, and Services) on a supported Cisco Unified IP phone. • To use a Cisco Unified Communications Manager directory as an external directory source, you must list the MAC addresses of the phones in Cisco Unified Communications Manager and reset the phones from Cisco Unified Communications Manager. You do not need to assign ephone-dns to the phones for the phones to register with Cisco Unified Communications Manager. • The **url services** command is also available in ephone-template configuration mode. If you use an ephone template to provision the Services feature button on one or more SCCP phones and you configure the **url services** command in telephony-service configuration mode, the value set in telephony-service configuration mode appears first in the list of options displayed when the phone user presses the Services feature button.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

What to Do Next

If you want to create an ephone template to provision multiple URLs for the Services feature button on supported individual SCCP phones, see Templates, on page 1427.

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Provision URLs for Feature Buttons on SIP Phones

To customize URLs for feature buttons in the SEPDEFAULT.cnf configuration profile for SIP IP phones, perform the following steps.

Restriction

- Operation of these services is determined by the Cisco Unified IP phone capabilities and the content of the specified URL.
- Provisioning the directory URL to select an external directory resource disables the Cisco Unified CME local directory service.

Before You Begin

Cisco CME 3.4 or a later version.

Support for **idle** *url* is available only on Unified CME 12.0 and later versions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **url** {**authentication** | **directory** | **service** | **idle**} *url*
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.

	Command or Action	Purpose
Step 3	**voice register global** **Example:** `Router(config)#`	Enters telephony-service configuration mode.

Step 4	**url** {**authentication** | **directory** | **service** | **idle**} *url*
	
	Example:
	`Router(config-register-global)# url directory http://10.0.0.11/localdirectory`
	`Router(config-register-global)# url service http://10.0.0.4/CCMUser/123456/urltest.html`
	`Router(config-register-global)# url idle http://www.mycompany.com/files/logo.xml idle-timeout 12`
		Associates a URL with the programmable feature buttons on SIP phones.
		• **url authentication** *url* — Uses the information at the specified URL to validate requests made to the phone web server.
		• **url directory** *url* — Uses the information at the specified URL for the Directories button display.
		• **url service** *url* [**root**] — Uses the information at the specified URL for the Services button display.
		• **url idle** *url* — Defines the location of a file to display on phones that are not in use and specifies the interval between refreshes of the display, in seconds.

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

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Profiles for SIP Phones, on page 391.

Troubleshooting URL Provisioning for Feature Buttons

Ensure the HTTP server is enabled and that there is communication between the Cisco Unified CME router and the server.

Modify Vendor Parameters for All SCCP Phones

To configure programmable phone and display parameters in the vendorConfig section of the SepDefault.conf.xml configuration file for all phones, perform the following steps.

Restriction

- Only the parameters supported by the currently loaded firmware are available.
- The number and type of parameters may vary from one firmware version to the next.
- Only those parameters that are supported by a Cisco Unified IP phone and firmware version are implemented. Parameters that are not supported are ignored.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **service phone** *parameter-name parameter-value*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

Step 4	**service phone** *parameter-name parameter-value*
	
	Example:
	`Router(config-telephony)# service phone daysDisplayNotActive 1,2,3,4,5,6,7`
	`Router(config-telephony)# service phone displayOnTime 07:30`
	`Router(config-telephony)# service phone displayOnDuration 10:00`
	`Router(config-telephony)# service phone displayIdleTimeout 00.01`
		Sets display and phone functionality for all IP phones that support the configured parameters and to which this template is applied.
		• The parameter name is word and case-sensitive. See Cisco Unified CME Command Reference for a list of parameters.
		• This command can also be configured in ephone-template configuration mode and applied to one or more phones.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Modify Vendor Parameters for a Specific SCCP Phone

To configure parameters in the vendorConfig section of the Sep*.conf.xml configuration file for an individual SCCP phone, perform the following steps.

Restriction

- Cisco Unified CME 4.0 or a later version.
- System must be configured to for per-phone configuration files. For configuration information, see Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- Only the parameters supported by the currently loaded firmware are available.
- The number and type of parameters may vary from one firmware version to the next.
- Only those parameters that are supported by a Cisco Unified IP phone and firmware version are implemented. Parameters that are not supported are ignored.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **service phone** *parameter-name parameter-value*
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone-template** *template-tag* **Example:** `Router (config)# ephone-template 15`	Enters ephone-template configuration mode to create an ephone template.

Step 4	**service phone** *parameter-name parameter-value*
	
	Example:
	`Router(config-telephony)# service phone daysDisplayNotActive 1,2,3,4,5,6,7`
	`Router(config-telephony)# service phone displayOnTime 07:30`
	`Router(config-telephony)# service phone displayOnDuration 10:00`
	`Router(config-telephony)# service phone displayidleTimeout 00.01`
		Sets parameters for all IP phones that support the configured functionality and to which this template is applied.
		• The parameter name is word and case-sensitive. See the Cisco Unified CME Command Reference for a list of parameters.
		• This command can also be configured in telephony-service configuration mode. For individual phones, the template configuration for this command overrides the system-level configuration for this command.

Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits from this command mode to the next highest mode in the configuration mode hierarchy.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 15`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Exits configuration mode and enters privileged EXEC mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Troubleshooting Vendor Parameter Configuration

Step 1 Ensure that the templates have been properly applied to the phones.

Step 2 Ensure that you use the **create cnf-files** command to regenerate configuration files and reset the phones after you apply the templates.

Step 3 Use the **show telephony-service tftp-bindings** command to display the configuration files that are associated with individual phones

Example:

```
Router# show telephony-service tftp-binding

    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/XMLDefault7960.cnf.xml alias SEP00036B54BB15.cnf.xml
    tftp-server system:/its/germany/7960-font.xml alias German_Germany/7960-font.xml
    tftp-server system:/its/germany/7960-dictionary.xml alias German_Germany/7960-dictionary.xml
    tftp-server system:/its/germany/7960-kate.xml alias German_Germany/7960-kate.xml
    tftp-server system:/its/germany/SCCP-dictionary.xml alias German_Germany/SCCP-dictionary.xml
    tftp-server system:/its/germany/7960-tones.xml alias Germany/7960-tones.xml
```

Step 4 Use the **debug tftp events** command to verify that the phone is accessing the file when you reboot the phone.

Configure One-Way Push-to-Talk on Cisco Unified SCCP Wireless IP Phones

To associate a phone button with the thumb button on a wireless phone for one-way Push-to-Talk (PTT) functionality in Cisco Unified CME, perform the following steps.

Restriction Supported on Cisco Unified Wireless IP Phone 7921 and 7925 only.

Before You Begin

- Cisco Unified CME 7.0 or a later version.
- Cisco phone firmware version 1.0.4 or a later version.

- System must be configured to for per-phone configuration files. For configuration information, see Define Per-Phone Configuration Files and Alternate Location for SCCP Phones, on page 181.
- Phone button to be associated with the thumb button must be configured with an intercom DN that targets a paging number. For configuration information, see Intercom Lines, on page 783.
- Paging group to be dialed by the intercom line must be configured. Targeted paging group can be unicast or multicast or both. For configuration information, see Paging, on page 857.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **service phone thumbButton1 PTTH** *button_number*
5. **exit**
6. **ephone** *phone-tag*
7. **ephone-template** *template-tag*
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	**ephone-template** *template-tag* **Example:** `Router (config)# ephone-template 12`	Enters ephone-template configuration mode to create an ephone template.
Step 4	**service phone thumbButton1 PTTH** *button_number* **Example:** `Router(config-ephone-template)# service phone thumbButton1 PTTH6`	Specifies which button is to go off hook when user presses the thumb button. • *button_number*—Button on phone that is configured with an intercom dn that targets a paging number. Range is 1 to 6. • There are no spaces in the **PTTH** and *button_number* keyword/argument combination. • This command can also be configured in telephony-service configuration mode. For individual phones, the template

	Command or Action	Purpose
		configuration for this command overrides the system-level configuration for this command.
Step 5	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits from this command mode to the next highest mode in the configuration mode hierarchy.
Step 6	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode.
Step 7	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 12`	Applies an ephone template to the ephone that is being configured.
Step 8	**end** **Example:** `Router(config-ephone)# end`	Exits configuration mode and enters privileged EXEC mode.

Configure Cisco Jabber for CSF Client in Cisco Unified CME

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http secure-server**
4. **ip http secure-port** *port number*
5. **voice register dn** *dn-tag*
6. **number** *number*
7. **voice register pool** *phone-tag*
8. **id device-id-name**
9. **type** *type*
10. **number** *number*
11. **username** *username* **password** *password*
12. **description** *string*
13. **exit**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip http secure-server** **Example:** `Router(config)# ip http secure-server`	Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) Version 3 protocol.
Step 4	**ip http secure-port** *port number* **Example:** `Router(config)# ip http secure-port 8443`	Sets the HTTPS server port number for listening.
Step 5	**voice register dn** *dn-tag* **Example:** `Router(config)# voice register dn 1`	Creates directory numbers for the SIP IP phones that are directly connected to Cisco Unified CME
Step 6	**number** *number* **Example:** `Router(config-register-dn)# number 991001`	Defines the numbers for the SIP IP phones.
Step 7	**voice register pool** *phone-tag* **Example:** `Router# voice register pool 1`	Sets the phone type for the SIP IP phones on a Cisco Unified CME system.
Step 8	**id device-id-name** **Example:** `Router(config-register-pool)# id device-id-name JabberWIN`	Specifies the device ID of a phone type. For a list of supported device IDs, see Cisco Unified Communications Manager Express Command Reference. Assigns a name to a phone type. • *name*—String that specifies the SIP soft client device ID name. Device ID name string can be up to 32 characters.

	Command or Action	Purpose
Step 9	**type** *type* **Example:** `Router(config-register-pool)# type Jabber-CSF-Client`	Defines the phone type.
Step 10	**number** *number* **Example:** `Router(config-register-pool)# number 1`	Defines the numbers for the SIP IP phones.
Step 11	**username** *username* **password** *password* **Example:** `Router(config-register-pool))# username jabber1 password jabber1`	Sets the username and password. • *Username*— Specifies the username of the phone type. • *Password*— Specifies the password of the phone type.
Step 12	**description** *string* **Example:** `Router(config-register-pool)# description Jabber-CSF-Client`	Associates a description with the Cisco Jabber client. Enter a string of up to 64 characters. A maximum of 128 characters, including spaces.
Step 13	**exit** **Example:** `Router(config-register-pool)# exit`	Exits the voice register-pool configuration mode.
Step 14	**end** **Example:** `Router(config)# end`	Exits the privileged EXEC configuration mode.

What to Do Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Configuration Examples for Cisco Unified IP Phone Options

Example for Configuring Cisco Jabber

The following example shows phone type Cisco Jabber configured under voice register pool 10:

```
!
voice register dn  10
```

```
  number 1089
  call-forward b2bua busy 1500
  call-forward b2bua mailbox 1500
  call-forward b2bua noan 1500 timeout 20
  pickup-call any-group
  pickup-group 1
  name CME SIP iPhone
  label CME SIP iPhone
 !
 !
 voice register pool  8
 registration-timer max 720 min 660
  park reservation-group 1
  session-transport tcp
  type CiscoMobile-iOS
  number 1 dn 10
  dtmf-relay rtp-nte
 !
 ephone-dn  61
  number 1061
  park-slot reservation-group 1 timeout 10 limit 2 recall retry 2 limit 2
 !
```

Example for Configuring Cisco Jabber CSF Client

The following example shows how to configure the Cisco Jabber CSF client installed in full UC mode:

```
!
voice register dn 1
number 991001
name Jabber-CSF-Client-1
label   Jabber-CSF-Client-1
!
voice register pool 1
id device-id-name jabber_csf_1
type Jabber-CSF-Client
number 1 dn 1
username john password john123
codec g711ulaw
camera
video
!
ip http secure-server
ip http secure-port 8443
```

The following example shows how to configure the Cisco Jabber CSF client in phone-only mode from CME under voice register global:

```
voice register global
 phone-mode phone-only
!
voice register pool  1
 id device-id-name winJabber
 number 1 dn 1
 type Jabber-CSF-Client
 username 1111022 password 1111022
!
```

The following example shows how to configure the Cisco Jabber CSF client in phone-only mode from CME under voice register pool:

```
 voice register pool  1
 id device-id-name winJabber
 number 1 dn 1
 type Jabber-CSF-Client
 username 1111022 password 1111022
```

```
 phone-mode phone-only
!
```

The following example shows how to configure the Cisco Jabber CSF client in phone-only mode from CME under voice register template:

```
voice register template  1
 phone-mode phone-only
!
voice register pool  2
 id device-id-name winJabber
 type Jabber-CSF-Client
 number 1 dn 2
 username 1111023 password 1111023
 template 1
!
```

Example for Configuring Dial Rules for Cisco Softphone SIP Client

The following example shows dial rules configured under voice register template 2:

```
!
voice register template  2
 url ldapServer ldap.abcd.com
 url AppDialRule tftp://10.1.1.1/AppDialRules.xml
 url DirLookupRule tftp://10.1.1.1/DirLookupRules.xml
!
```

The following is a sample of Application Dial Rule content:

```
Router#more flash:AppDialRules.xml
<?xml version="1.0" encoding="UTF-8"?><DialRules<
        <DialRule BeginsWith="+1" NumDigits="12" DigitsToRemove="1" PrefixWith="9"/>
        <DialRule BeginsWith="+1" NumDigits="12" DigitsToRemove="1" PrefixWith="9"/>
        <DialRule BeginsWith="919" NumDigits="10" DigitsToRemove="3" PrefixWith="9"/>
        <DialRule BeginsWith="1" NumDigits="11" DigitsToRemove="0" PrefixWith="9"/>
        <DialRule BeginsWith="" NumDigits="10" DigitsToRemove="0" PrefixWith="91"/>
        <DialRule BeginsWith="" NumDigits="7" DigitsToRemove="0" PrefixWith="9"/>
        <DialRule BeginsWith="+" NumDigits="13" DigitsToRemove="1" PrefixWith="9011"/>
        <DialRule BeginsWith="+" NumDigits="14" DigitsToRemove="1" PrefixWith="9011"/>
        <DialRule BeginsWith="+" NumDigits="15" DigitsToRemove="1" PrefixWith="9011"/>


        <DialRule BeginsWith="+" NumDigits="12" DigitsToRemove="1" PrefixWith="9011"/>
        <DialRule BeginsWith="+" NumDigits="11" DigitsToRemove="1" PrefixWith="9011"/>
</DialRules>
```

Example for Excluding Local Services from Cisco Unified SIP IP Phones

The following example shows how the **exclude** command is used to exclude from the Cisco Unified SIP IP phone's user interface the availability of two local services. These services are Local Directory and My Phone Apps.

```
Router(config)# voice register pool 80
Router(config-register-pool)# exclude directory
Router(config-register-pool)# exclude myphoneapps
```

Example to Create Text Labels for Ephone-dns

The following example creates text labels for two ephone-dns:

```
ephone-dn 1
 number 2001
 label Sales
ephone-dn 2
 number 2002
 label Engineering
```

Example for Phone Header Bar Display

The following example provides the full E.164 number for a phone line in the phone header bar:

```
ephone-dn 55
 number 2149
 description 408-555-0149
ephone-dn 56
 number 2150
ephone 12
 button 1:55 2:56
```

Example for System Text Message Display

The following example specifies text that should display on IP phones when they are not in use:

```
telephony-service
 system message ABC Company
```

Example for System File Display

The following example specifies that a file called logo.htm should be displayed on IP phones when they are not in use:

```
telephony-service
 url idle http://www.abcwrecking.com/public/logo.htm idle-timeout 35
```

Example for URL Provisioning for Directories, Services, and Messages Buttons

The following example provisions the Directories, Services, and Messages buttons:

```
telephony-service
 url directories http://10.4.212.4/localdirectory
 url services http://10.4.212.4/CCMUser/123456/urltest.html
 url messages http://10.4.212.4/Voicemail/MessageSummary.asp
```

Example for Programmable VendorConfig Parameters

The following partial output shows a template in which programmable parameters for phone and display functionality have been configured by using the **service phone** command:

```
ephone-template 1
 button-layout 7931 1
 service phone daysDisplayNotActive 1,2,3,4,5,6,7
 service phone backlightOnTime 07:30
 service phone backlightOnDuration 10:00
 service phone backlightidleTimeout 00.01
```

In the following example, the PC port is disabled on phones 26 and 27. All other phones have the PC port enabled.

```
ephone-template  8
 service phone pcPort 1
!
!
ephone  26
 mac-address 1111.1111.1001
 ephone-template 8
 type 7960
 button  1:26
!
!
ephone  27
 mac-address 1111.2222.2002
 ephone-template 8
 type 7960
 button  1:27
```

Example for Push-to-Talk (PTT) on Cisco Unified Wireless IP Phones in Cisco Unified CME

The following partial output shows a template in which one-way PTT is configured by using the **service phone thumbButton1** command:

```
ephone-template 12
service phone thumbButton1 PTTH6
!
    !
    ephone-dn 10
    intercom 1050
    ephone-dn 50
    number 1050
    paging
    !
    !

ephone 1
type 7921
   button 1:1 6:10
!
!
ephone 2
    button 1:2
    paging-dn 50
    ephone 3
    button 1:3
    paging-dn 50
```

```
ephone 4
button 1:1
paging-dn 50
```

Feature Information for Cisco Unified IP Phone Options

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

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

Table 112: Feature Information for Cisco Unified IP Phone Options

Feature Name	Cisco Unified CME Version	Feature Information
My Phone Apps for Cisco Unified SIP IP Phones	9.0	Adds support for My Phone Apps feature on Cisco Unified SIP IP phones.
Support for Cisco Jabber	8.6	Added support for Cisco Jabber.
Clear Directory Entries	8.6	Provides ability to clear the display of call-history details such as missed, placed, and received call entries on a Cisco Unified SCCP IP phone's display screen.
Fixed Line/Feature Buttons	4.0(2)	Provides two preconfigured fixed sets of feature buttons for provisioning a Cisco Unified IP Phone 7931G.
Header Bar Display	3.4	Added support for modifying header bar display on SIP phones.
	2.01	Phone header bar display is introduced.
Labels for Directory Numbers	3.4	Added support for label display on SIP phones.
	3.0	Ephone-dn labels were introduced.

Feature Name	Cisco Unified CME Version	Feature Information
Programmable Vendor Parameters	4.0	Added support for configuring programmable phone and display functionality at a phone level for SCCP phones.
	3.4	Added support for configuring programmable phone and display functionality for SIP phones.
	3.2.1	Added support for programmable phone and display functionality in vendorConfig portion of configuration file. Implementation of configuration is firmware version dependent.
System Message Display	3.0	System message display on idle phones using text messages was introduced.
	2.1	System message display on idle phones using HTML files was introduced.
URL Provisioning for Feature Buttons	12.0	Added support for Idle URL functionality on SIP phones.
	4.2	Added support for configuring an ephone template to provision multiple URLs for the Services feature button phones.
	3.4	Added support for provisioning customized URLs for programmable feature buttons on supported SIP phones.
	2.0	Provisioning customized URLs for programmable feature buttons was introduced.

CHAPTER 49

Interoperability with Cisco Unified CCX

This chapter describes features in Cisco Unified Communications Manager Express (Cisco Unified CME) that provide support for interoperability between Cisco Unified CME and external feature services, such as Cisco Customer Response Solutions (CRS) with Cisco Unified Contact Center Express (Cisco Unified CCX).

Note To configure support for computer-based CSTA client applications, such as a Microsoft Office Communicator (MOC) client or an application developed by using the Cisco Unified CME CTI SDK, see Configure CTI CSTA Protocol Suite, on page 1521.

Information About Interoperability with Cisco Unified CCX

Cisco Unified CME 4.2 and later versions support interoperability between Cisco Unified CME and Cisco Customer Response Solutions (CRS) with Cisco Unified Call Center Express (Cisco Unified CCX), including enhanced call processing, device and call monitoring, unattended call transfers to multiple call center agents and basic extension mobility, and IP IVR applications.

The Cisco Unified CCX application uses the CRS platform to provide a multimedia (voice, data, and web). Cisco IP IVR functionality is available with Cisco Unified CCX and includes prompt-and-collect and call treatment.

The following functions are provided in Cisco Unified CME 4.2 and later versions:

- Support of Cisco Unified CCX Cisco Agent Desktop for use with Cisco Unified CME
- Configuration query and update between Cisco Unified CCX and Cisco Unified CME
- SIP-based simple and supplementary call control services including:
    - Call routing between Cisco Unified CME and Cisco Unified CCX using SIP-based route point

    - First-party call control for SIP-based simple and supplementary calls
    - Call monitoring and device monitoring based on SIP presence and dialog event package

- Cisco Unified CCX session management of Cisco Unified CME
- Cisco Unified CCX device and call monitoring of agent lines and call activities in Cisco Unified CME

Provisioning and configuration information in Cisco Unified CCX is automatically provided to Cisco United CME. If the configuration from Cisco Unified CCX is deleted or must be modified, you can configure the same information in Cisco Unified CME by using Cisco IOS commands.

For first party call control, a route point for Cisco CRS is a peer device to Cisco Unified CME through a SIP trunk. An incoming call to Cisco Unified CME that is targeted to a call center phone is routed to Cisco Unified CCX through the route point. The call is placed in a queue and redirected to the most suitable agent by Cisco Unified CCX.

Supplementary services such as call hold, blind transfer, and semi-attended transfer are initiated by Cisco Unified CCX. Existing SIP-based simple and supplementary service call flow applies except for blind transfers. For blind transfers with Cisco Unified CCX as the transferrer, Cisco Unified CCX will stay in the active state until the transfer target answers. It drops out only after the transferred call is successfully answered. If the transfer target does not answer when ringing times out, the call is pulled back by Cisco Unified CCX and rerouted to another agent. This mechanism also applies when the transfer target is configured with call-forward all or forward no-answer. The forward configuration is ignored during blind transfer.

When a call moves between Cisco Unified CCX and Cisco Unified CME because of redirect, transfer, and conference, the SIP Call-ID continues to change. For call control purposes, Cisco Unified CME issues a unique Global Call ID (Gcid) for every outbound call leg. A Gcid remains the same for all legs of the same call in the system, and is valid for redirect, transfer, and conference events, including 3-party conferencing when a call center phone acts as a conference host.

Before Cisco IOS Release 12.4(11)XW6, if the call monitoring module in Cisco Unified CME 4.2 detected a call associated with a non default session application, such as B-ACD or a TCL script, the module was globally disabled. After the module was disabled, Cisco Unified CCX administration had to manually re-enable the call monitoring module after the session completes.

In Cisco IOS Release 12.4(11)XW6 and later releases, the call monitoring module in Cisco Unified CME does not monitor a call associated with a non default session application, such as B-ACD or a TCL script, including all calls merged into this call by way of consult transfer and conference. The module is not disabled and continues to monitor other calls.

Table 113: Tasks to Configure Interoperability between Cisco CRS and Cisco Unified CME, on page 1497 contains a list of tasks required to enable operability between Cisco Unified CME and Cisco Unified CCX, presented in the order in which the tasks are to be completed. This section contains information about performing tasks in the first 2 steps in this table and procedures for completing step 3.

For configuration information, see Configure Interoperability with Cisco Unified CCX, on page 1498.

Table 113: Tasks to Configure Interoperability between Cisco CRS and Cisco Unified CME

Step	Task	Name of Document
1	Verify that the appropriate Cisco Unified Communications Manager Express (Cisco Unified CME) version is installed on the router. For compatibility information, see Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide.	—
2	Configure the Cisco Unified CME router. **Tip** Note the XML user ID and password in Cisco Unified CME and router's IP address.	See "Prerequisites' section in Enable Interoperability with Cisco Unified CCX, on page 1498.
3	Configure Cisco Unified CME to enable interoperability with Cisco Unified CCX.	Configure Interoperability with Cisco Unified CCX, on page 1498
4	Install Cisco Unified Contact Center Express (Cisco Unified CCX) for Cisco Unified CME.	See *Cisco Unified Contact Center Express Administration Guide* at Configuration Guides.
5	Perform the initial setup of Cisco CRS for Cisco Unified CME. **Tip** When setup launches, you are asked for the XML user ID and password, known as AXL user in Cisco CRS, that you created in Cisco Unified CME. You also must enter the router IP address.	
6	Configure Cisco Unified CME telephony subsystem to enable interoperability with Cisco Unified CCX.	"*Provisioning Unified CCX for Unified CME*" chapter in the appropriate *Cisco CRS Administration Guide* or *Cisco Unified Contact Center Express Administration Guide* at Configuration Guides.
7	Create users and assign the agent capability in Cisco CRS.	

Configure Interoperability with Cisco Unified CCX

Enable Interoperability with Cisco Unified CCX

To configure Cisco Unified CME to enable interoperability between Cisco Unified CME and Cisco Unified CCX, perform the following steps.

Note A single Cisco Unified CME can support multiple session managers.

Restriction

- Maximum number of *active* Cisco Unified CCX agents supported: 50.
- Multi-Party Ad Hoc and Meet-Me Conferencing are not supported.
- The following incoming calls are supported for deployment of the interoperability feature: SIP trunk calls from another Cisco Unified CME and all calls from a PSTN trunk. Other trunks, such H.323, are supported as usual in Cisco Unified CME, however, not for customer calls to Cisco Unified CCX.

Before You Begin

- Cisco Unified CME version and Cisco IOS release that is compatible with your Cisco Unified CCX version. For compatibility information, see Cisco Unified Contact Center Express (Cisco Unified CCX) Software and Hardware Compatibility Guide.
- XML API must be configured to create an AXL username for Cisco Unified CCX access. For configuration information, see Configure the XML API, on page 1573.

  Note During the initial setup of Cisco CRS for Cisco Unified CME, you need the AXL username and password that was configured using the **xml user** command in telephony-service configuration mode. You also need the router IP address that was configured using the **ip source-address** command in telephony-service configuration mode.

- Agent phones to be connected in Cisco Unified CME must be configured in Cisco Unified CME. When configuring a Cisco Unified CCX agent phone, use the **keep-conference endcall** command to enable conference initiators to exit from conference calls and end the conference for the remaining parties. For configuration information, see Configure Conferencing, on page 1377.
- The Cisco Unified CME router must be configured to accept incoming presence requests. For configuration information, see Configure Presence Service, on page 879.
- To support Desktop Monitoring and Recording, the **service phone SpanToPCPort 1** command must be configured in telephony-service configuration mode. For configuration information, see Modify Vendor Parameters for All SCCP Phones, on page 1479.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice call send-alert**
4. **voice service voip**
5. **callmonitor**
6. **gcid**
7. **allow-connections sip to sip**
8. **no supplementary-service sip moved-temporary**
9. **no supplementary-service sip refer**
10. **sip**
11. **registrar server**[**expires** [**max** *sec*] [**min** *sec*]]
12. **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 call send-alert** **Example:** `Router(config)# voice call send-alert`	Enables the terminating gateway to send an alert message instead of a progress message after it receives a call setup message.
Step 4	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode and specifies voice-over-IP encapsulation.
Step 5	**callmonitor** **Example:** `Router(config-voi-serv)# callmonitor`	Enables call monitoring messaging functionality. • Used by Cisco Unified CCX for processing and reporting.
Step 6	**gcid** **Example:** `Router(config-voi-serv)# gcid`	Enables Global Call-ID (Gcid) for call control purposes. • Used by Cisco Unified CCX for tracking call.

	Command or Action	Purpose
Step 7	**allow-connections sip to sip** **Example:** `Router(config-voi-serv)# allow-connections sip to sip`	Allows connections between specific types of endpoints in a VoIP network.
Step 8	**no supplementary-service sip moved-temporary** **Example:** `Router(config-voi-serv)# no supplementary-service sip moved-temporary`	Prevents the router from sending a redirect response to the destination for call forwarding.
Step 9	**no supplementary-service sip refer** **Example:** `Router(config-voi-serv)# no supplementary-service sip refer`	Prevents the router from forwarding a REFER message to the destination for call transfers.
Step 10	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 11	**registrar server**[**expires** [**max** *sec*] [**min** *sec*]] **Example:** `Router(config-voi-sip)# registrar server expires max 600 min 60`	Enables SIP registrar functionality in Cisco Unified CME. • **expires**—(Optional) Sets the active time for an incoming registration. • **max** *sec*—(Optional) Maximum time for a registration to expire, in seconds. Range: 600 to 86400. Default: 3600. Recommended value: 600. **Note** Ensure that the registration expiration timeout is set to a value smaller than the TCP connection aging timeout to avoid disconnection from the TCP. • **min** *sec*—(Optional) Minimum time for a registration to expire, in seconds. Range: 60 to 3600. Default: 60.
Step 12	**end** **Example:** `Router(config-voi-serv)# end`	Exits configuration mode and enters privileged EXEC mode.

Identify Agent Directory Numbers in Cisco Unified CME for Session Manager on SCCP Phones

To specify which directory numbers, associated with phone lines on Cisco Unified CCX agent phones, can be managed by a session manager, perform the following steps.

Restriction

- Only SCCP phones can be configured as agent phones in Cisco Unified CME. The Cisco VG224 Analog Phone Gateway and analog and SIP phones are supported as usual in Cisco Unified CME, however, not as Cisco Unified CCX agent phones.
- Cisco Unified IP Phone 7931 cannot be configured as an agent phone in Cisco Unified CME. Cisco Unified IP Phone 7931s are supported as usual in Cisco Unified CME, however, not as Cisco Unified CCX agent phones.
- Shared-line appearance is not supported on agent phones. A directory number cannot be associated with more than one physical agent phone at one time.
- Overlaid lines are not supported on agent phones. More than one directory number cannot be associated with a single line button on an agent phone.
- Monitored mode for a line button is not supported on agent phones. An agent phone cannot be monitored by another phone.
- Cisco Unified CCX does not support a call event that includes a different directory number; all call events must include the primary directory number. Call transfers between phones with single-line directory numbers will cause call monitoring to fail.

Before You Begin

- Up to eight session managers must be configured in Cisco Unified CME.
- Directory numbers associated with Cisco Unified CCX agent phones must be configured in Cisco Unified CME.
    - Cisco Unified CME 4.2: Directory numbers for agent phones must be configured as dual lines to allow an agent to make two call connections at the same time using one phone line button. Note that if the second line of the dual-line directory number is busy, a transfer event between phones in the solution will fail to complete.
    - Cisco Unified CME 4.3/7.0 and later versions: We recommend that directory numbers for agent phones be configured as octal lines to help to ensure that a free line with the same directory number is available for a transfer event.
    - For configuration information, see Configure Phones to Make Basic Call, on page 315.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **allow watch**
5. **session-server** *session-server-tag* [**,...***session-server-tag*]
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	**ephone-dn** *dn-tag* **Example:** `Router(config)# ephone-dn 24`	Enters ephone-dn configuration mode. • *dn-tag*—Unique ID of an already configured directory number. The tag number corresponds to a tag number created when this directory number was initially configured.
Step 4	**allow watch** **Example:** `Router(config-ephone-dn)# allow watch`	Allows the phone line associated with this directory number to be monitored by a watcher in a presence service. • This command can also be configured in ephone-dn template configuration mode and applied to one or more phones. The ephone-dn configuration has priority over the ephone-dn template configuration.
Step 5	**session-server** *session-server-tag* [**,...***session-server-tag*] **Example:** `Router(config-ephone-dn)# session-server 1,2,3,4,6`	Specifies which session managers are to monitor the directory number being configured. • *session-server-tag*—Unique ID session manager, configured in Cisco Unified CCX and automatically provided to Cisco Unified CME. Range: 1 to 8. **Tip** If you do not know the value for *session-server-tag*, we recommend using 1. • Can configure up to eight session-server-tags; individual tags must be separated by commas (**,**). • Each directory number can be managed by up to eight session managers. Each session manager can monitor more than one directory number.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

Verify Registrations and Subscriptions in Cisco Unified CME

Before using the system, verify registrations and subscriptions for Cisco Unified CCX endpoints.

Step 1 Use the **show sip status registrar** command to verify whether session manager and Cisco CRS route points are registered.

Step 2 Use the **show presence subscription summary** command to verify whether Cisco CRS route points and Cisco Unified CCX agent directory numbers are subscribed.

The following is sample output from the **show presence subscription summary** command. The first two rows show the status for two route points. The next two are for logged in agent phones.

```
Router# show presence subscription summary

Presence Active Subscription Records Summary: 15 subscription
Watcher                  Presentity               SubID Expires SibID  Status
======================== ======================== ====== ======= ====== ======
CRScontrol@10.4.171.81   8101@10.4.171.34         4      3600    0      idle
CRScontrol@10.4.171.81   8201@10.4.171.34         8      3600    0      idle
CRScontrol@10.4.171.81   4016@10.4.171.34         10 3600    0      idle
CRScontrol@10.4.171.81   4020@10.4.171.34         12 3599    0      idle
```

Re-create a Session Manager in Cisco Unified CME

Note Provisioning and configuration information in Cisco Unified CCX is automatically provided to Cisco United CME. The following task is required only if the configuration from Cisco Unified CCX is deleted or must be modified.

To re-create a session manager in Cisco Unified CME for Cisco Unified CCX, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register session-server** *session-server-tag*
4. **register id** *name*
5. **keepalive** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register session-server** *session-server-tag* **Example:** `Router(config)# voice register session-server 1`	Enters voice register session-server configuration mode to enable and configure a session manager for an external feature server, such as the Cisco Unified CCX application on a Cisco CRS system. • Range: 1 to 8. • A single Cisco Unified CME can support multiple session managers.
Step 4	**register id** *name* **Example:** `Router(config-register-fs)# CRS1`	(Optional) Required only if the configuration from Cisco Unified CCX is deleted or must be modified. • *name*—String for identifying Cisco Unified CCX. Can contain 1 to 30 alphanumeric characters.
Step 5	**keepalive** *seconds* **Example:** `Router(config-register-fs)# keepalive 300`	(Optional) Required only if the configuration from Cisco Unified CCX is deleted or must be modified. • Keepalive duration for registration, in seconds, after which the registration expires unless Cisco Unified CCX reregisters before the registration expiry. • Range: 60 to 3600. Default: 300. **Note** Default in Cisco Unified CCX is 120.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-register-fs)# end`	Exits configuration mode and enters privileged EXEC mode.

Reconfigure a Cisco CRS Route Point as a SIP Endpoint

Note Provisioning and configuration information in Cisco Unified CCX is automatically provided to Cisco United CME. The following task is required only if the configuration from Cisco Unified CCX is deleted or must be modified.

To reconfigure a Cisco CRS route point as a SIP endpoint in Cisco Unified CME, perform the following steps.

Restriction

- Each Cisco CRS route point can be managed by only one session manager.
- Each session manager can manage more than one Cisco CRS route point.

Before You Begin

- Directory numbers associated with Cisco CRS route points must be configured in Cisco Unified CME. For configuration information for directory numbers associated with SIP endpoints, see Configure Phones to Make Basic Call, on page 315.
- Directory numbers associated with Cisco CRS route points must be enabled to be watched. For configuration information, see Configure Presence Service, on page 879.
- The **mode cme** command must be enabled in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *number*
5. **session-server** *session-server-tag* [**,...***session-server-tag*]
6. **allow watch**
7. **refer target dial-peer**
8. **exit**
9. **voice register pool** *pool-tag*
10. **number** *tag* **dn** *dn-tag*
11. **session-server** *session-server-tag*
12. **codec** *codec-type*
13. **dtmf-relay sip-notify**
14. **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 register dn** *dn-tag* **Example:** `Router(config-register-global)# voice register dn 1`	Enters voice register dn configuration mode to define a directory number for a SIP phone, intercom line, voice port, or a message-waiting indicator (MWI).
Step 4	**number** *number* **Example:** `Router(config-register-dn)# number 2777`	Defines a valid number for a directory number.
Step 5	**session-server** *session-server-tag* [**,...***session-server-tag*] **Example:** `Router(config-register-dn)# session-server 1`	Specifies which session managers are to monitor the directory number being configured. • *session-server-tag*—Unique ID session manager, configured in Cisco Unified CCX and automatically provided to Cisco Unified CME. Range: 1 to 8.

	Command or Action	Purpose
		Tip If you do not know the value for *session-server-tag*, we recommend using 1. • Can configure up to eight session-server-tags; individual tags must be separated by commas (**,**). • Each directory number can be managed by up to eight session managers. Each session manager can monitor more than one directory number.
Step 6	**allow watch** **Example:** `Router(config-register-dn)# allow watch`	Allows the phone line associated with this directory number to be monitored by a watcher in a presence service.
Step 7	**refer target dial-peer** **Example:** `Router(config-register-dn)# refer target dial-peer`	Enables watcher to handle SIP REFER message from this directory number. • **target dial-peer—**Refer To portion of message is based on address from dial peer for this directory number.
Step 8	**exit** **Example:** `Router(config-register-dn)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 9	**voice register pool** *pool-tag* **Example:** `Router(config)#` **voice register pool 3**	Enters voice register pool configuration mode to set device-specific parameters for a Cisco CRS route point. • A voice register pool in Cisco Unified CCX can contain up to 10 individual SIP endpoints. Subsequent pools are created for additional SIP endpoints.
Step 10	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 1`	Associates a directory number with the route point being configured.
Step 11	**session-server** *session-server-tag* **Example:** `Router(config-register-pool)# session-server 1`	identifies session manager to be used to control the route point being configured. • *session-server-tag***—**Unique number assigned to a session manager. Range: 1 to 8. The tag number corresponds to a tag number created by using the **voice register session-server** command.

	Command or Action	Purpose
Step 12	**codec** *codec-type* **Example:** `Router(config-register-pool)# codec g711ulaw`	Specifies the codec for the dial peer dynamically created for the route point being configured. • *codec-type*—g711ulaw is required for Cisco Unified CCX.
Step 13	**dtmf-relay sip-notify** **Example:** `Router(config-register-pool)# dtmf-relay sip-notify`	Specifies DTMF Relay method to be used by the route point being configured.
Step 14	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuration Examples for Interoperability with Cisco Unified CCX

The following output from the **show running-configuration** command shows the configuration on a Cisco Unified CME router that will interoperate with Cisco Unified CCX.

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sb-sj3-3845-uut1
!
boot-start-marker
boot-end-marker
!
card type t1 0 2
card type t1 0 3
logging buffered 1000000
no logging console
enable password password
!
no aaa new-model
network-clock-participate wic 2
network-clock-participate wic 3
ip cef
!
!
no ip dhcp use vrf connected
!
!
ip dhcp excluded-address 192.0.2.250 192.0.2.254
!
```

```
ip dhcp pool ephones
   network 192.0.2.0 255.255.255.0
   option 150 ip 192.0.2.254
   default-router 192.0.2.254
!
!
no ip domain lookup
!
isdn switch-type primary-5ess
voice-card 0
 no dspfarm
!
!
!
!
voice service voip
 gcid
 callmonitor
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 sip
  registrar server expires max 120 min 60
!
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
!
!
!
!
!
!
!
!
!
voice register global
 mode cme
 source-address 192.0.2.254 port 5060
 max-dn 720
 max-pool 240
 authenticate presence
 authenticate register
 dialplan-pattern 1 511.... extension-length 4
 voicemail 9001
 create profile sync 0000347600391314
!
voice register session-server  1
 keepalive 300
 register-id SB-SJ3-UCCX1_1164774025000
!
voice register dn  1
 session-server 1
 number 8999
 allow watch
 refer target dial-peer
!
voice register dn  2
 session-server 1
 number 8001
 allow watch
 refer target dial-peer
!
voice register dn  3
 session-server 1
 number 8101
 allow watch
 refer target dial-peer
```

```
!
voice register dn  11
 number 2011
 name ep-sip-1-11
 mwi
!
voice register dn  12
 number 2012
 name ep-sip-1-12
 mwi
!
voice register dn  16
 number 5016
 name rp-sip-1-16
 label SIP 511-5016
 mwi
!
voice register dn  17
 number 5017
 name rp-sip-1-17
 label SIP 511-5017
 mwi
!
voice register dn  18
 number 5018
 name rp-sip-1-18
 label SIP 511-5018
 mwi
!
voice register pool  1
 session-server 1
 number 1 dn 1
 number 2 dn 2
 number 3 dn 3
 dtmf-relay sip-notify
 codec g711ulaw
!
voice register pool  11
 id mac 1111.0711.2011
 type 7970
 number 1 dn 11
 dtmf-relay rtp-nte
 voice-class codec 1
 username 5112011 password 5112011
!
voice register pool  12
 id mac 1111.0711.2012
 type 7960
 number 1 dn 12
 dtmf-relay rtp-nte
 voice-class codec 1
 username 5112012 password 5112012
!
voice register pool  16
 id mac 0017.0EBC.1500
 type 7961GE
 number 1 dn 16
 dtmf-relay rtp-nte
 voice-class codec 1
 username rp-sip-1-16 password pool16
!
voice register pool  17
 id mac 0016.C7C5.0660
 type 7971
 number 1 dn 17
 dtmf-relay rtp-nte
 voice-class codec 1
 username rp-sip-1-17 password pool17
!
voice register pool  18
 id mac 0015.629E.825D
 type 7971
 number 1 dn 18
```

```
 dtmf-relay rtp-nte
 voice-class codec 1
 username rp-sip-1-18 password pool18
!
!
!
!
!
!
!
controller T1 0/2/0
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-4,24
!
controller T1 0/2/1
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-4,24
!
controller T1 0/3/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 0 timeslots 1-4 type e&-immediate-start
!
controller T1 0/3/1
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 0 timeslots 1-4 type e&-immediate-start
vlan internal allocation policy ascending
!
!
!
!
interface GigabitEthernet0/0
 ip address 209.165.201.1 255.255.255.224
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 192.0.2.254 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface Serial0/2/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Serial0/2/1:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
interface Service-Engine1/0
 ip unnumbered GigabitEthernet0/0
 service-module ip address 209.165.202.129 255.255.255.224
 service-module ip default-gateway 209.165.201.1
!
ip route 192.0.0.30 255.0.0.0 192.0.0.55
ip route 209.165.202.129 255.255.255.224 Service-Engine1/0
```

```
ip route 192.0.2.56 255.255.255.0 209.165.202.2
ip route 192.0.3.74 255.255.255.0 209.165.202.3
ip route 209.165.202.158 255.255.255.224 192.0.0.55
!
!
ip http server
ip http authentication local
ip http path flash:
!
!
ixi transport http
 response size 64
 no shutdown
 request outstanding 1
!
ixi application cme
 no shutdown
!
!
!
control-plane
!
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/2/0:23
!
voice-port 0/3/0:0
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/2/1:23
!
voice-port 0/3/1:0
!
!
!
!
!
dial-peer voice 9000 voip
 description ==> This is for internal calls to CUE
 destination-pattern 9...
 voice-class codec 1
 session protocol sipv2
 session target ipv4:209.165.202.129
 dtmf-relay rtp-nte sip-notify
!
dial-peer voice 9001 voip
 description ==> This is for external calls to CUE
 destination-pattern 5119...
 voice-class codec 1
 session protocol sipv2
 session target ipv4:209.165.202.129
 dtmf-relay rtp-nte sip-notify
!
dial-peer voice 521 voip
 destination-pattern 521....
 voice-class codec 1
 max-redirects 5
 session protocol sipv2
 session target ipv4:209.165.201.2
 dtmf-relay rtp-nte sip-notify
!
dial-peer voice 531 voip
 destination-pattern 531....
 voice-class codec 1
 max-redirects 5
 session protocol sipv2
```

```
 session target ipv4:209.165.201.3
 dtmf-relay rtp-nte sip-notify
!
!
presence
 presence call-list
 watcher all
 allow subscribe
!
sip-ua
 mwi-server ipv4:209.165.202.128 expires 3600 port 5060 transport udp
 presence enable
!
!
telephony-service
 no auto-reg-ephone
 xml user axluser password axlpass 15  <====AXL username and password for Cisco CRS
 max-ephones 240
 max-dn 720
 ip source-address 192.0.2.254 port 2000  <====IP address of router
 system message sb-sj3-3845-uut1
 url services http://192.0.2.252:6293/ipphone/jsp/sciphonexml/IPAgentInitial.jsp
 url authentication http:192.0.2.252:6293/ipphone/jsp/sciphonexml/IPAgentAuthenticate.jsp
 cnf-file perphone
 dialplan-pattern 1 511.... extension-length 4
 voicemail 9001
 max-conferences 8 gain -6
 call-forward pattern .T
 moh flash:music-on-hold.wav
 multicast moh 239.10.10.1 port 2000
 transfer-system full-consult
 transfer-pattern .T
 create cnf-files version-stamp 7960 Jun 18 2007 07:44:25
!
!
ephone-dn  1  dual-line
 session-server 1
 number 1001
 name ag-1-1
 allow watch
 mwi sip
!
!
ephone-dn  2  dual-line
 session-server 1
 number 1002
 name ag-1-2
 allow watch
 mwi sip
!
!
ephone-dn  3  dual-line
 session-server 1
 number 1003
 name ag-1-3
 allow watch
 mwi sip
!
!
ephone-dn  4  dual-line
 session-server 1
 number 1004
 name ag-1-4
 allow watch
 mwi sip
!
!
ephone-dn  5
 session-server 1
 number 1005
 name ag-1-5
 allow watch
 mwi sip
```

```
!
!
ephone-dn  11  dual-line
 number 3011
 name ep-sccp-1-11
 mwi sip
!
!
ephone-dn  12
 number 3012
 name ep-sccp-1-12
 mwi sip
!
!
ephone-dn  16  dual-line
 number 4016
 label SCCP 511-4016
 name rp-sccp-1-16
 mwi sip
!
!
ephone-dn  17  dual-line
 number 4017
 label SCCP 511-4017
 name rp-sccp-1-17
 mwi sip
!
!
ephone-dn  18  dual-line
 number 4018
 label SCCP 511-4018
 name rp-sccp-1-18
 mwi sip
!
!
ephone-dn  19  dual-line
 number 4019
 label SCCP 511-4019
 name rp-sccp-1-19
 mwi sip
!
!
ephone-dn  20  dual-line
 number 4020
 label SCCP 511-4020
 name rp-sccp-1-20
 mwi sip
!
!
ephone-dn  21  dual-line
 number 4021
 label SCCP 511-4021
 name rp-sccp-1-21
 mwi sip
!
!
ephone-dn  22  dual-line
 number 4022
 label SCCP 511-4022
 name rp-sccp-1-22
 mwi sip
!
!
ephone  1
 mac-address 1111.0711.1001
 type 7970
 keep-conference endcall
 button  1:1
!
!
!
ephone  2
 mac-address 1111.0711.1002
```

```
 type 7970
 keep-conference endcall
 button  1:2
!
!
!
ephone  3
 mac-address 1111.0711.1003
 type 7970
 keep-conference endcall
 button  1:3
!
!
!
ephone  4
 mac-address 1111.0711.1004
 type 7970
 keep-conference endcall
 button  1:4
!
!
!
ephone  5
 mac-address 1111.0711.1005
 type 7970
 keep-conference endcall
 button  1:5
!
!
!
ephone  11
 mac-address 1111.0711.3011
 type 7970
 keep-conference endcall
 button  1:11
!
!
!
ephone  12
 mac-address 1111.0711.3012
 type 7960
 keep-conference endcall
 button  1:12
!
!
!
ephone  16
 mac-address 0012.D916.5AD6
 type 7960
 keep-conference endcall
 button  1:16
!
!
!
ephone  17
 mac-address 0013.1AA6.7A9E
 type 7960
 keep-conference endcall
 button  1:17
!
!
!
ephone  18
 mac-address 0012.80F3.B013
 type 7960
 keep-conference endcall
 button  1:18
!
!
!
ephone  19
 mac-address 0013.1A1F.6282
 type 7970
```

```
 keep-conference endcall
 button  1:19
!
!
!
ephone  20
 mac-address 0013.195A.00D0
 type 7970
 keep-conference endcall
 button  1:20
!
!
!
ephone  21
 mac-address 0017.0EBC.147C
 type 7961GE
 keep-conference endcall
 button  1:21
!
!
!
ephone  22
 mac-address 0016.C7C5.0578
 type 7971
 keep-conference endcall
 button  1:22
!
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
 password lab
 login
!
scheduler allocate 20000 1000
!
end
```

Where to Go Next

If you are done modifying parameters for phones in Cisco Unified CME, generate a new configuration file and restart the phones. See Generate Configuration Files for Phones, on page 388.

Feature Information for Interoperability with Cisco Unified CCX

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

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

Table 114: Feature Information for Interoperability Feature

Feature Name	Cisco Unified CME Version	Modification
Interoperability with Cisco Unified CCX	4.2	Enables interoperability between Cisco Unified CME and Cisco Customer Response Solutions (CRS) 5.0 and later versions with Cisco Unified Contact Center Express (Cisco Unified CCX), including Cisco Unified IP IVR, enhanced call processing, device and call monitoring, unattended call transfers to multiple call center agents, and basic extension mobility.

CHAPTER 50

CTI CSTA Protocol Suite

This chapter describes how to configure the Computer Telephony Integration (CTI) Computer Supported Telecommunications Applications (CSTA) protocol suite in Cisco Unified Communications Manager Express (Cisco Unified CME) 8.0 and later versions to allow computer-based CSTA client applications, such as a Microsoft Office Communicator (MOC) client or an application developed using the Cisco Unified Communications Express (UC Express) Services Interface SDK, to monitor and control the Cisco Unified CME system and enable programmatic control of SCCP telephony devices registered in Cisco Unified CME.

Note To configure support for interoperability between Cisco Unified CME and Cisco Customer Response Solutions (CRS) with Cisco Unified Contact Center Express (Cisco Unified CCX), see Configure Interoperability with Cisco Unified CCX, on page 1498.

Information About CTI CSTA Protocol Suite

CTI CSTA in Cisco Unified CME

The CTI CSTA Protocol Suite in Cisco Unified CME 8.0 and later versions provides third-party call-control capabilities for computer-based CSTA client applications, such as a Microsoft Office Communicator (MOC) client through Microsoft Office Communications Server (OCS) and applications created using the Cisco Unified CME CTI SDK, and enables click-to-dial from the application.

The CTI CSTA Protocol Suite in Cisco Unified CME 8.8 and later versions enables the dial-via-office functionality from the application.

CSTA Client Application Deployment

Typically, a computer-based application uses CSTA to control its associated PBX phone via a SIP CSTA gateway. The gateway terminates SIP messages and converts ECMA-323 messages to and from the PBX-specific protocol.

In Cisco Unified CME 8.0 and later versions, a computer-based CSTA client application interacts directly with Cisco Unified CME via the CTI interface in Cisco Unified CME to control and monitor IP phones registered in Cisco Unified CME. Cisco Unified CME replaces the CSTA gateway and the PBX in the typical application-to-PBX deployment to terminate SIP messages from the client application and convert CSTA XML into the line-side protocol that controls the phone.

CTI Session

If required, a CSTA client application creates a session by establishing a SIP dialog with the CTI interface in Cisco Unified CME 8.0 and later versions. The logical name of the phone user is described in the SIP "From" header while the PBX phone line is described in the SIP "To" header. The user and line configurations are created in the application.

The SIP INVITE body includes a System Status service request. A SIP "OK" response that includes a System Status response is sent from Cisco Unified CME. The application continues only if it receives the expected response.

After receiving the expected response, the client application begins the capabilities exchange by sending a SIP message requesting a list of supported CSTA services and events from Cisco Unified CME. Cisco Unified CME sends a response with an encapsulated CSTA features response that is a list of supported services and events. For information, see Supported Services and Events, on page 1520.

The CSTA client application must start a CSTA monitor before it can observe changes to calls and features by CSTA events. To start the Call Monitor Module (CMM) in Cisco Unified CME, the application sends a SIP INFO message with an encapsulated service request. The CTI interface authorizes this request and sends back a SIP 200 OK response with an encapsulated ECMA-323 Monitor Start response. After this, Cisco Unified CME starts generating subsequent events in SIP INFO messages to the application.

During a CTI session, the CSTA client application sets a timer (default: 30 minutes) in the INVITE message and refreshes it via RE-INVITE message. Cisco Unified CME deletes a SIP dialog after the session expires.

Supported Services and Events

Table 115: Supported CSTA Services and Events, on page 1521 lists CSTA services and events that are supported by the CTI CSTA protocol Suite in Cisco Unified CME 8.0 and later versions. Not all CSTA client applications can support all features. For more information, see the user documentation for your CSTA client application.

Table 115: Supported CSTA Services and Events

Function	Supported Services and Events
Call Control	• Make Call • Answer Call • Clear Connection • Reconnect • Hold Call • Retrieve Call (Resume) • Deflect Call (only at alerting state) • Single Step Transfer Call • Consultation Call • Transfer Call • Alternate Call Generate Digits (DTMF)
Logical Phone Features	• Get Do Not Disturb • Set Do Not Disturb • Get CFwdALL • Set CFwdAll
Physical Device	Set MWI
Snapshot Services	Snapshot Device

For a complete list of the services and events supported by the CTI CSTA Protocol Suite, see *UCX-SI SDK Developer's Guide* at: http://developer.cisco.com/web/ucxapi/docs.

Configure CTI CSTA Protocol Suite

Table 116: Tasks to Configure Interoperability Between a CSTA Client Application and Cisco Unified CME, on page 1522 contains a list of tasks required to enable a computer-based CSTA client application to control IP phones in Cisco Unified CME, presented in the order in which the tasks are to be completed. This document contains information about performing tasks in the first 2 steps in this table and procedures for completing step 3.

Table 116: Tasks to Configure Interoperability Between a CSTA Client Application and Cisco Unified CME

Step	Task	Name of Document
1	Verify that the appropriate version of Cisco Unified Communications Manager Express (Cisco Unified CME) is installed on the router.	-
2	Configure Cisco Unified CME including AXL user name and password for the computer-based CSTA client application, if required. **Tip** Take note of the AXL user ID and password of the application and the IP address of the Cisco Unified CME router. **Note** An AXL credential is not required for a MOC client.	See 'Prerequisites' in Enable CTI CSTA in Cisco Unified CME, on page 1522.
3	Configure Cisco Unified CME to enable interoperability with CSTA client application.	See the configuration procedures.
4	Install CSTA client application.	See documentation for your application.
5	Configure CSTA client application for Cisco Unified CME, including SIP URI of CTI gateway front-end or client application.	

Enable CTI CSTA in Cisco Unified CME

To configure Cisco Unified CME to enable interoperability between Cisco Unified CME and a computer-based CSTA client application, perform the following steps.

Note During the initial setup of the CSTA client application, you need the router IP address configured using the **ip source-address** command in telephony-service configuration mode. For some client applications, you may also need the AXL username and password configured using the **xml user** command in telephony-service configuration mode.

Before You Begin

- Cisco Unified CME 8.0 or a later version must be installed and configured on the Cisco router.

- (Not required for a MOC client) XML API must be configured to create an AXL username for some CSTA client application access. To determine if an AXL username is required for your application, see your application documentation. For configuration information, see Configure the XML API, on page 1573.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections sip-to-sip**
5. **no supplementary-service sip moved-temporary**
6. **no supplementary-service sip refer**
7. **no cti shutdown**
8. **callmonitor**
9. **gcid**
10. **cti csta mode basic**
11. **cti message device-id suppress-conversion**
12. **sip**
13. **registrar server** [**expires**[**max** *sec*][**min***sec*]]
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode and specifies voice-over-IP encapsulation.
Step 4	**allow-connections sip-to-sip** **Example:** `Router(config-voi-serv)# allow-connections sip-to-sip`	Allows connections between specific types of endpoints in a VoIP network.

	Command or Action	Purpose
Step 5	**no supplementary-service sip moved-temporary** **Example:** `Router(config-voi-serv)# no supplementary-service sip moved-temporary`	Disables supplementary service for call forwarding.
Step 6	**no supplementary-service sip refer** **Example:** `Router(config-voi-serv)# no supplementary-service sip refer`	Prevents the router from forwarding a REFER message to the destination for call transfers.
Step 7	**no cti shutdown** **Example:** `Router(config-voi-serv)# no cti shutdown`	Enables CTI integration.
Step 8	**callmonitor** **Example:** `Router(config-voi-serv)# callmonitor`	(Optional) Enables call monitoring messaging functionality for processing and reporting. • This command is *not* required for a MOC client.
Step 9	**gcid** **Example:** `Router(config-voi-serv)# gcid`	(Optional) Enables Global Call-ID (Gcid) for call control purposes. • This command is *not* required for a MOC client.
Step 10	**cti csta mode basic** **Example:** `Router(config-voi-serv)# cti csta mode basic`	(Optional) Suppresses enhanced feature/extension in CTI messages. • Required for a MOC client.
Step 11	**cti message device-id suppress-conversion** **Example:** `Router(config-voi-serv)# cti message device-id suppress-conversion`	(Optional) Suppresses conversion or promotion of extension numbers of associated endpoints in CTI messages. • This command is *not* required for a MOC client.
Step 12	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode. • Required only if you perform the following step for enabling the SIP registrar function in Cisco Unified CME.
Step 13	**registrar server** [**expires**[**max** *sec*][**min***sec*]] **Example:** `Router(config-voi-sip)# registrar server expires max 600 min 60`	(Optional) Enables SIP registrar functionality in Cisco Unified CME. • **max***sec*—(Optional) Maximum time for a registration to expire, in seconds. Range: 600 to 86400. Default: 3600. Recommended value: 600.

	Command or Action	Purpose
		Note Ensure that the registration expiration timeout is set to a value smaller than the TCP connection aging timeout to avoid disconnection from the TCP. • This command is *not* required for a MOC client.
Step 14	**end** **Example:** `Router(config-voi-sip)# end`	Exits voice-service configuration mode and enters privileged EXEC mode.

Examples

The following example shows the required configuration for supporting interaction with a MOC client:

```
voice service voip
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 no cti shutdown
 cti csta mode basic
!
!
!
```

What to Do Next

- If you are configuring a CSTA client application that requires a session server in Cisco Unified CME, go to Create a Session Manager, on page 1525.
- If you are configuring Cisco Unified CME to interact with a MOC client, go to Configure a Number or Device for CTI CSTA Operations, on page 1527.

Create a Session Manager

To configure a session manager in Cisco Unified CME for a CSTA client application, perform the following steps.

Note

- This task is *not* required for a MOC client.
- A single Cisco Unified CME can support multiple session managers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode cme**
5. **exit**
6. **voice register session-server** *session-server-tag*
7. **cti-aware**
8. **register-id** *name*
9. **keepalive** *seconds*
10. **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 register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 4	**mode cme** **Example:** `Router(voice-register-global)# mode cme`	Enables mode for provisioning SIP devices in Cisco Unified CME.
Step 5	**exit** **Example:** `Router(voice-register-global)# configure terminal`	Exits to global configuration mode.
Step 6	**voice register session-server** *session-server-tag* **Example:** `Router(config)# voice register session-server 1`	Enters voice register session-server configuration mode to enable and configure a session manager. • Range: 1 to 8. • A single Cisco Unified CME can support multiple session managers.

	Command or Action	Purpose
Step 7	**cti-aware** **Example:** `Router(config-register-fs)# cti-aware`	Binds this session manager to the CTI subsystem and enables CTI-specific Register heartbeat.
Step 8	**register-id** *name* **Example:** `Router(config-register-fs)# register app1`	Creates an ID for explicitly identifying the CSTA client application during Register requests. • *name*—String for identifying application. Can contain 1 to 30 alphanumeric characters.
Step 9	**keepalive** *seconds* **Example:** `Router(config-register-fs)# keepalive 60`	Keepalive duration for registration, in seconds, after which the registration expires unless the application reregisters before the registration expiry. • Range: 60 to 3600. Default: 300.
Step 10	**end** **Example:** `Router(config-register-fs)# end`	Exits voice register session-server configuration mode and enters privileged EXEC mode.

Examples

```
!
voice register global
 mode cme
 source-address 10.0.0.1 port 5060
!
!
voice register session-server  1
 keepalive 60
 register-id app1
 cti-aware
!
```

Configure a Number or Device for CTI CSTA Operations

To configure a directory number or an IP phone for CTI CSTA operations, perform the following steps for each number or phone to be monitored and controlled by the CSTA client application.

Restriction

- Only SCCP IP phones can be controlled by a CSTA client application. The Cisco VG224 Analog Phone Gateway and analog and SIP phones are supported as usual in Cisco Unified CME but not as IP phones for a CSTA client application.
- Overlay DNs are not supported on IP phones for a CSTA client application. The Call Monitor Module in Cisco Unified CME is unable to determine if two inbound calls to the same directory number are on the same phone or on different phones, as in an overlay configuration. Overlays DNs are supported as usual in Cisco Unified CME but not on IP phones to be controlled or monitored by a CSTA client application.
- Not all SCCP IP phones support the Prompted Make Call feature in the CTI CSTA protocol suite. The Cisco VG224 Analog Phone Gateway, Cisco ATAs, and SCCP-controlled FXS ports on Cisco routers do not support a prompted make-call request from a CSTA client application. Certain Cisco Unified phone models, including the Cisco Unified 792X and Cisco Unified 793X, may be unable to complete a prompted make-call request from a CSTA client application.
- Prompted Make Call is not supported on IP phones associated with a MOC Client. Prompted Make Call is supported as usual in Cisco Unified CME but not on IP phones to be controlled by a MOC client.
- Shared lines are not supported on an IP phone associated with a MOC client. Shared lines are supported as usual in Cisco Unified CME but not on IP phones to be controlled by a MOC client.
- If the phone to be controlled and monitored by a MOC client is an Extension Mobility (EM) phone, the MOC client must log into the phone using the credential in an EM user profile when no users are logged into the EM phone or after an EM user logs in.

Before You Begin

- Directory number or IP phone to be controlled and monitored by the application is configured in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.
- Extension Mobility (EM) phone to be controlled and monitored by the application must be configured in Cisco Unified CME, including the required user profiles. For information, see Extension Mobility, on page 725.

SUMMARY STEPS

1. **enable**
2. **emadmin login** *name ephone-tag*
3. **emadmin logout** *name*
4. **configure terminal**
5. **ephone-dn** *tag*
6. **cti watch**
7. **cti notify**
8. **exit**
9. **telephony-service**
10. **em external**
11. **url services** *url* **root**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**emadmin login** *name ephone-tag* **Example:** `Router# emadmin login user204 2`	(Optional) Enables application to log in to an IP phone that is enabled for Extension Mobility. • *name*—Credential in EM user profile configured with the **user** (voice user-profile) command. • *ephone-tag*—identifier for IP phone that is enabled for Extension Mobility. Required for a MOC client if the MOC client will control the number or device to be configured.
Step 3	**emadmin logout** *name* **Example:** `Router# emadmin logout user204`	(Optional) Logs the application out of the Extension Mobility phone. • *name*—Credential in Extension Mobility that the application used to log into an Extension Mobility phone.
Step 4	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 5	**ephone-dn** *tag* **Example:** `Router(config)# ephone-dn 1`	Enters ephone-dn configuration mode.
Step 6	**cti watch** **Example:** `Router(config-ephone-dn)# cti watch`	Allows this directory number to be monitored and controlled by a CSTA client application. • This command can also be configured in ephone-dn-template configuration mode. The value set in ephone-dn configuration mode has priority over the value set in ephone-dn-template mode.
Step 7	**cti notify** **Example:** `Router(config-ephone-dn)# cti notify`	(Optional) Forces ephone-dn into constant "up" state to allow CTI operations on this directory number. • Required if ephone-dn to be monitored/controlled is not associated with a physical device. • This command can also be configured in ephone-dn-template configuration mode. The value set in ephone-dn configuration mode has priority over the value set in ephone-dn-template mode.
Step 8	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 9	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode. • Required only if you perform Step 10 to Step 11 for configuring the Services menu on an IP phone.
Step 10	**em external** **Example:** `Router(config-telephony)# em external`	(Optional) Removes login page for Extension Mobility from the Services menu on IP phones.
Step 11	**url services** *url* **root** **Example:** `Router(config-telephony)# url services http://my_application/menu.html root`	(Optional) Provides menu of root phone services under the Services button on IP phones. • *url*—URL for external menu of root phone services provided by an application.
Step 12	**end** **Example:** `Router(config-telephony)# end`	Exits telephony-service configuration mode and enters privileged EXEC mode.

Examples

```
!
voice logout-profile 1
 number 203 type normal
!
voice user-profile 1
 user user204 password psswrd
 number 204 type normal
!
.
.
.
ephone-dn  1
 number 201
 cti watch
!
!
ephone-dn  2
 number 202
 cti watch
!
!
ephone-dn  3
 number 203
 cti watch
!
!
ephone-dn  4
 number 204
 cti notify
 cti watch
!
!
ephone  1
 mac-address 001E.4A34.A35F
 type 7961
 button  1:1
!
!
!
ephone  2
 mac-address 000F.8FC7.B681
 type 7960
 button  1:2
!
!
!
ephone  3
 mac-address 0019.E7FF.1E30
 type 7961
 logout-profile 1
```

Clear a Session Between a CSTA Client Application and Cisco Unified CME

To gracefully tear down a CTI session between a CSTA client application and Cisco Unified CME, perform the following steps.

Before You Begin

- Cisco Unified CME 8.0 or a later version.
- Determine the session ID using the **show cti session** command.

SUMMARY STEPS

1. **enable**
2. **clear cti session id** *session-tag*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear cti session id** *session-tag* **Example:** `Router# clear cti session id 3`	Clears the session between a CSTA client application and Cisco Unified CME.

Configuration Examples for CTI CSTA Protocol Suite

Example for Configuring MOC Client

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sdatar-2811s
!
boot-start-marker
boot system flash c2800nm-ipvoice-mz.oct_20090510
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
ip source-route
!
!
ip cef
!
ip dhcp pool test
   network 10.0.0.0 255.255.255.0
   option 150 ip 10.0.0.1
   default-router 10.0.0.1
!
!
no ipv6 cef
multilink bundle-name authenticated
!
```

```
!
voice service voip
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 no cti shutdown
 cti csta mode basic
!
!
!
!
voice logout-profile 1
 number 203 type normal
!
voice user-profile 1
 user user204 password psswrd
 number 204 type normal
!
voice-card 0
!
!
!
archive
 log config
  hidekeys
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Service-Engine0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 1.5.41.5 255.255.0.0
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.1.43.254
ip route 223.255.254.254 255.255.255.255 1.5.0.1
!
!
ip http server
!
!
ixi transport http
 response size 64
 no shutdown
 request outstanding 1
 request timeout 60
!
ixi application cme
 no shutdown
!
!
!
control-plane
!
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/0/2
!
voice-port 0/0/3
!
```

```
!
mgcp fax t38 ecm
!
!
!
sip-ua
!
!
telephony-service
 em logout 1:0
 max-ephones 10
 max-dn 100
 ip source-address 10.0.0.1 port 2000
 cnf-file location flash:
 cnf-file perphone
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
ephone-dn  1
 number 201
 cti watch
!
!
ephone-dn  2
 number 202
 cti watch
!
!
ephone-dn  3
 number 203
 cti watch
!
!
ephone-dn  4
 number 204
 cti notify
 cti watch
!
!
ephone  1
 mac-address 001E.4A34.A35F
 type 7961
 button  1:1
!
!
!
ephone  2
 mac-address 000F.8FC7.B681
 type 7960
 button  1:2
!
!
!
ephone  3
 mac-address 0019.E7FF.1E30
 type 7961
 logout-profile 1
```

Example for Configuring CSTA Client Application Requiring a Session Manager

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sdatar-2811s
!
```

```
boot-start-marker
boot system flash c2800nm-ipvoice-mz.oct_20090510
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
ip source-route
!
!
ip cef
!
ip dhcp pool test
   network 10.0.0.0 255.255.255.0
   option 150 ip 10.0.0.1
   default-router 10.0.0.1
!
!
no ipv6 cef
multilink bundle-name authenticated
!
!
voice service voip
 no cti shutdown
 csta cti mode basic
 sip
  registrar server expires max 120 min 60
!
voice register global
 mode cme
 source-address 10.0.0.1 port 5060
!
voice register session-server  1
 keepalive 60
 register-id apps
 cti-aware
!
!
voice logout-profile 1
 number 203 type normal
!
voice user-profile 1
 user user204 password cisco
 number 204 type normal
!
!
!
voice-card 0
!
!
!
archive
 log config
  hidekeys
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Service-Engine0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 1.5.41.5 255.255.0.0
 duplex auto
 speed auto
!
ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 10.1.43.254
ip route 223.255.254.254 255.255.255.255 1.5.0.1
!
!
ip http server
!
!
ixi transport http
 response size 64
 no shutdown
 request outstanding 1
 request timeout 60
!
ixi application cme
 no shutdown
!
!
!
control-plane
!
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/0/2
!
voice-port 0/0/3
!
!
mgcp fax t38 ecm
!
!
!
!
sip-ua
!
!
telephony-service
 em logout 1:0
 max-ephones 10
 max-dn 100
 ip source-address 10.0.0.1 port 2000
 cnf-file location flash:
 cnf-file perphone
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-dn  1
 number 201
 cti watch
!
!
ephone-dn  2
 number 202
 cti watch
!
!
ephone-dn  3
 number 203
 cti watch
!
!
ephone-dn  4
 number 204
 cti notify
 cti watch
!
!
ephone  1
```

```
 mac-address 001E.4A34.A35F
 type 7961
 button  1:1
!
!
!
ephone  2
 mac-address 000F.8FC7.B681
 type 7960
 button  1:2
!
!
!
ephone  3
 mac-address 0019.E7FF.1E30
 type 7961
 logout-profile 1
!
!
!
```

Feature Information for CTI CSTA Protocol Suite

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

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

Table 117: Feature Information for CTI CSTA Protocol Suite

Feature Name	Cisco Unified CME Version	Feature Information
CTI CSTA Protocol Suite Enhancement	8.8	Enables the dial-via-office functionality from computer-based CSTA client applications and adds support to CSTA services and events.

Feature Name	Cisco Unified CME Version	Feature Information
CTI CSTA Protocol Suite in Cisco Unified CME	8.0	Introduces industry-standard Computer Telephony Integration (CTI) interface that enables computer-based CSTA client applications to interact directly with Cisco Unified CME to monitor/control IP phones. The following commands are new or modified for this feature:**clear csta session**, **cti-aware**, **cti csta mode**, **cti message device-id suppress-conversion**, **cti notify**,**cti shutdown**, **cti watch**, **debug cti**,**debug cti callmon**, **emadmin login**, **emadmin logout**,**em external**, **show cti**, **url (telephony-service)**

CHAPTER 51

SRST Fallback Mode

Prerequisites for SRST Fallback Mode

- The IP address of the Cisco Unified CME router must be registered as the SRST reference on the Cisco Unified Communications Manager device pool.
- Cisco Unified CME 4.0 or a later version must be installed on the Cisco Unified CME router that is configured in SRST mode.
- Following tasks must be completed:
    - Generate Configuration Files for Phones, on page 388
    - Configure System-Level Parameters, on page 167. Note that the **max-dn** command must be explicity configured with the **preference** keyword to support calls between PSTN and IP phones during SRST fallback mode.
    - Configure Call Transfer and Forwarding, on page 1178

Restrictions for SRST Fallback Mode

- The **call-manager-fallback** command, which is used to configure Cisco Unified SRST, cannot be used on a router that is configured for Cisco Unified CME.
- The **telephony-service setup** command and **auto assign** command must not be enabled on a Cisco Unified CME router configured for SRST fallback mode. If you used the **telephony-service setup**

command before configuring the router for SRST fallback support, you must remove any unwanted ephone directory numbers created by the setup process.

- The number of phones that fall back to a Cisco Unified CME router in SRST mode cannot exceed the maximum number of phones that is supported by the router. To find the maximum number of phones for a particular router and Cisco Unified CME version, see the appropriate *Cisco CME Supported Firmware, Platforms, Memory, and Voice Products* document at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_device_support_tables_list.html.
- The ephone-dns and ephones that are created from fallback may have less information associated with them than appears in their original configuration on a Cisco Unified Communications Manager or on an active Cisco Unified CME system. This situation occurs because the Cisco Unified CME router in SRST mode is designed to learn only a limited amount of information from the fallback IP phones. For example, if an ephone-dn has in its configuration the command **number 4888 no-reg** (to keep that extension from registering under its E.164 address), after fallback the **no-reg** part of this command will be lost because this information cannot be learned from the IP phones.
- The order of the SRST fallback ephone-dns and ephones will be different from the order of the active Cisco Unified Communications Manager or Cisco Unified CME ephone-dns and ephones. For example, ephone 1 on an active Cisco Unified Communications Manager might be numbered ephone 5 on the Cisco Unified CME router in SRST mode, because the order of learned ephone-dns and ephones is determined by the sequence of the ephone fallback occurrence, which is random.

Information About SRST Fallback Mode

SRST Fallback Mode Using Cisco Unified CME

This feature enables routers to provide call-handling support for Cisco Unified IP phones if they lose connection to remote primary, secondary, or tertiary Cisco Unified Communications Manager installations or if the WAN connection is down. When Cisco Unified SRST functionality is provided by Cisco Unified CME, provisioning of phones is automatic and most Cisco Unified CME features are available to the phones during periods of fallback, including hunt-groups, call park and access to Cisco Unity voice messaging services using SCCP protocol. The benefit is that Cisco Unified Communications Manager users will gain access to more features during fallback without any additional licensing costs.

This feature offers a limited telephony feature set during fallback mode. Customers who require the following features should continue to use Cisco Unified SRST, because these features are not supported with SRST fallback support using Cisco Unified CME.

- More than 240 phones during fallback service
- Cisco VG 248 Analog Phone Gateway support
- Secure voice fallback during SRST fallback service
- Simple, one-time configuration for SRST fallback service

Cisco Unified Communications Manager supports Cisco Unified IP phones at remote sites attached to Cisco Integrated Services Routers across the WAN. This new feature combines the many features available in Cisco Unified CME with the ability to automatically detect IP phone configurations that is available in Cisco Unified SRST to provide seamless call handling when communication with the Cisco Unified Communications Manager is interrupted.

When the system automatically detects a failure, Cisco Unified SRST uses Simple Network Auto Provisioning (SNAP) technology to auto-configure a branch office router to provide call processing for the Cisco Unified 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 returns to the primary Cisco Unified Communications Manager.

A limited number of phone features are automatically detected at the time that call processing falls back to Cisco Unified CME in SRST Fallback Mode, and an advantage of SRST fallback support using Cisco Unified CME is that you can choose to prebuild a Cisco Unified CME configuration that contains a number of extensions (ephone-dns) with additional features that you want them to have for some or all of your extensions. The configurations will contain ephone-dn configurations but will not identify which phones (which MAC addresses) will be associated with which ephone-dns (extension numbers).

By copying and pasting a prebuilt configuration onto Cisco Unified CME routers at several locations, you can use the same overall configuration for sites that are identically laid out. For example, if you have a number of retail stores, each with five to ten checkout registers, you can use the same overall configuration in each store. You might use a range of extensions from 1101 to 1110. Stores with fewer than ten registers will simply not use some of the ephone-dn entries you provide in the configuration. Stores with more extensions than you have prebuilt will use the auto-provisioning feature to populate their extra phones. The only configuration variations from store to store will be the specific MAC addresses of the individual phones, which are added to the configurations at the time of fallback.

When a phone registers for SRST service with a Cisco Unified CME router and the router discovers that the phone was configured with a specific extension number, the router searches for an existing prebuilt ephone-dn with that extension number and then assigns that ephone-dn number to the phone. If there is no prebuilt ephone-dn with that extension number, the Cisco Unified CME system automatically creates one. In this way, extensions without prebuilt configurations are automatically populated with extension numbers and features as the numbers and features are "learned" by the Cisco Unified CME router in SRST mode when the phone registers to the router after a WAN link fails.

The SRST fallback support using Cisco Unified CME feature is able to interrogate phones to learn their MAC addresses and the extension-to-ephone relationships associated with each phone. This information is used to dynamically create and execute the Cisco Unified CME **button** command for each phone and automatically provision each phone with the extensions and features you want it to have.

The following sequence describes how Cisco Unified CME provides SRST services for Cisco Unified Communications Manager phones when they lose connectivity with the Cisco Unified Communications Manager and fall back to the Cisco Unified CME router in SRST mode:

Before Fallback

1. Phones are configured as usual in Cisco Unified Communications Manager.
2. The IP address of the Cisco Unified CME router is registered as the SRST reference on the Cisco Unified Communications Manager device pool.
3. SRST mode is enabled on the Cisco Unified CME router.
4. (Optional) Ephone-dns and features are prebuilt on the Cisco Unified CME router.

During Fallback

1. Phones that are enabled for fallback register to the default Cisco Unified CME router that has SRST mode enabled. Each display-enabled IP phone displays the message that has been defined using the **system message** command under telephony-service configuration mode. By default, this message is "`Cisco Unified CME`."

2 While the fallback phones are registering, the router in SRST mode initiates an interrogation of the phones in order to learn their phone and extension configurations. The following information is acquired or "learned" by the router:

- MAC address
- Number of lines or buttons
- Ephone-dn-to-button relationship
- Speed-dial numbers

3 The option defined with the **srst mode auto-provision** command determines whether Cisco Unified CME adds the learned phone and extension information to its running configuration. If the information is added, it appears in the output when you use the **show running-config** command and is saved to NVRAM when you use the **write** command.

- Use the **srst mode auto-provision none** command to enable the Cisco Unified CME router to provide SRST fallback services for Cisco Unified Communications Manager.
- If you use the **srst mode auto-provision dn** or **srst mode auto-provision all** commands, the Cisco Unified CME router includes the phone configuration it learns from Cisco Unified Communications Manager in its running configuration. If you then save the configuration, the fallback phones are treated as locally configured phones on the Cisco Unified CME-SRST router which could adversely impact the fallback behavior of those phones.

4 While in fallback mode, Cisco Unified IP phones periodically attempt to reestablish a connection with Cisco Unified Communications Manager every 120 seconds (default). To manually reestablish a connection to Cisco Unified Communications Manager you can reboot the Cisco Unified IP phone.

5 When a connection is reestablished with Cisco Unified Communications Manager, Cisco Unified IP phones automatically cancel their registration with the Cisco Unified CME router in SRST mode. However, if a WAN link is unstable, Cisco Unified IP phones can bounce between Cisco Unified Communications Manager and the Cisco Unified CME router in SRST mode.

An IP phone connected to the Cisco Unified CME-SRST router over a WAN reconnects itself to Cisco Unified Communications Manager as soon as it can establish a connection to Cisco Unified Communications Manager over the WAN link. However, if the WAN link is unstable, the IP phone switches back and forth between Cisco Unified CME-SRST and Cisco Unified Communications Manager, causing temporary loss of phone service (no dial tone). These reconnect attempts, known as WAN link flapping issues, continue until the IP phone successfully reconnects itself back to Cisco Unified Communications Manager.

WAN link disruptions can be classified into two types: infrequent random outages that occur on an otherwise stable WAN, and sporadic, frequent disruptions that last a few minutes.

To resolve WAN-link flapping issues between Cisco Unified Communications Manager and SRST, Cisco Unified Communications Manager provides an enterprise parameter and a setting in the Device Pool Configuration window called Connection Monitor Duration. (Depending on system requirements, the administrator decides which parameter to use.) The value of the parameter is delivered to the IP phone in the XML configuration file.

- Use the enterprise parameter to change the connection duration monitor value for all IP phones in the Cisco Unified Communications Manager cluster. The default for the enterprise parameter is 120 seconds.
- Use the Device Pool Configuration window to change the connection duration monitor value for all IP phones in a specific device pool.

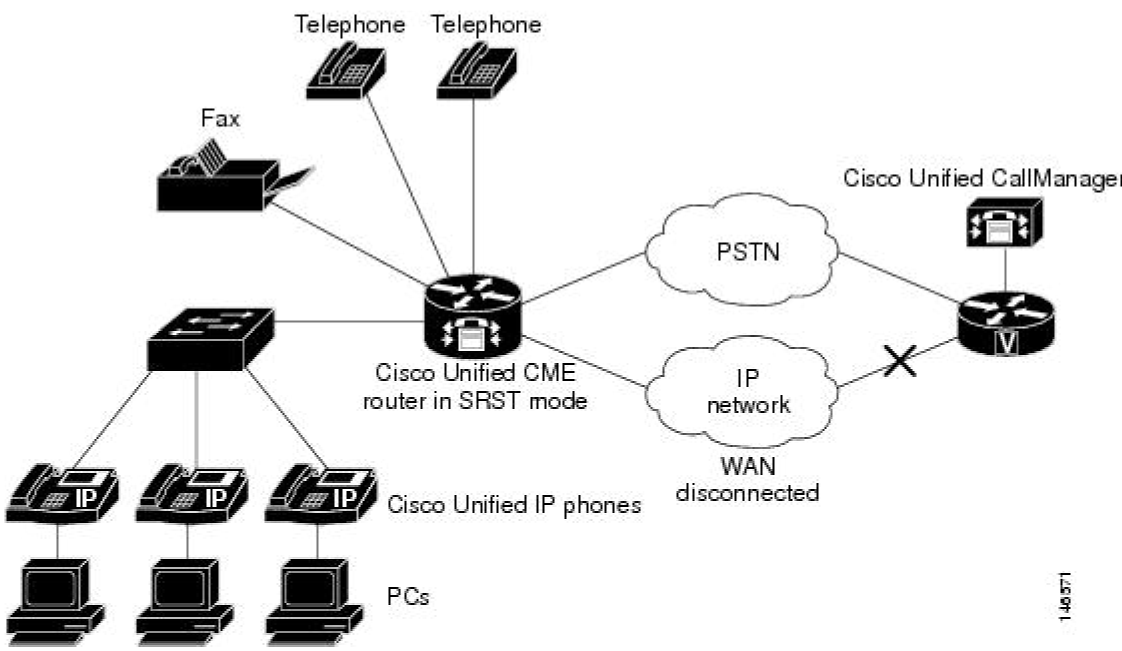
A Cisco Unified IP phone will not reestablish a connection with the primary Cisco Unified Communications Manager at the central office if it is engaged in an active call.

After the First Fallback

Additional features can be set up, such as ephone hunt groups, which can contain learned extensions and prebuilt extensions. The complete core set of Cisco Unified CME phone features is available to the IP phones and extensions, whether they are learned or configured.

Figure 71: SRST Fallback Support using Cisco Unified CME shows a branch office with several Cisco Unified IP phones connected to a Cisco Unified CME router in SRST fallback mode. 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. Cisco Unified CME provides SRST services for the phones when connectivity over the WAN link is interrupted.

Figure 71: SRST Fallback Support using Cisco Unified CME



Prebuilding Cisco Unified CME Phone Configurations

Prebuilding Cisco Unified CME ephone-dns allows you to create a set of directory numbers with extension numbers and some features, which will provide service during fallback that is similar to the service that is provided during normal operation. You can prebuild all of your normal extensions, a limited set of your extensions, or none of your extensions. Directory numbers that are not prebuilt will be populated with extension numbers and features as they are “learned” by the Cisco Unified CME router in SRST mode at the time of fallback.

An ephone-dn is the IP equivalent of a normal phone line in most cases. It represents a potential call connection and is associated with a virtual voice port and virtual dial peer. An ephone-dn has one or more extension or telephone numbers associated with it, which allow call connections to be made. An ephone-dn can be single-line, which allows one call connection to be made at a time, or dual-line, which allows two simultaneous call connections. Dual-line ephone-dns are useful for features such as call transfer or call waiting, in which one call is put on hold to connect to another. Single-line ephone-dns are required for certain features such as intercom, paging, and message-waiting indication (MWI). For more information, see Cisco Unified CME Overview, on page 67.

If an ephone-dn is manually configured in Cisco Unified CME, incoming calls will always route to the manually configured ephone-dn in Cisco Unified CME rather than to Cisco Unified Communications Manager using the voip dial peer. To avoid incorrect routing, configure a higher preference for the voip dial peer than the preference for the prebuilt directory number. For configuration example, see Example for Prebuilding DNs, on page 1552.

Auto provision Directory Numbers in SRST Fallback Mode

Cisco Unified CME 4.3 and later versions support octo-line directory numbers in SRST fallback mode. You can specify whether Cisco Unified CME in SRST fallback mode creates octo-line or dual-line directory numbers based on the phone type. For the Cisco Unified IP Phone 7902 or 7920, or an analog phone connected to the Cisco VG224 or Cisco ATA, the system creates a dual-line directory number; it creates an octo-line directory number for all other phone types. This applies only to the ephone-dns that are "learned" automatically from ephone configuration information, and not to ephone-dns that are manually configured in Cisco Unified CME.

Configure SRST Fallback Mode

Enable SRST Fallback Mode

Restriction Do not enable the **telephony-service setup** command or **auto assign** command on a Cisco Unified CME router that you are configuring for SRST fallback mode. If you used the **telephony-service setup** command previously on the router, you must remove any unwanted ephone directory numbers created by the setup process.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **srst mode auto-provision** {**all** | **dn** | **none**}
5. **srst dn line-mode** {**dual** | **dual-octo** | **octo** | **single**}
6. **srst dn template** *template-tag*
7. **srst ephone template** *template-tag*
8. **srst ephone description** *string*
9. **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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**srst mode auto-provision** {**all** | **dn** | **none**} **Example:** `Router(config-telephony)# srst mode auto-provision none`	Enables SRST mode for a Cisco Unified CME router. • **all**—Includes information for learned ephones and ephone-dns in the running configuration. • **dn**—Includes information for learned ephone-dns in the running configuration. • **none**—Does not include information for learned ephones or learned ephone-dns in the running configuration. Use this keyword when you want Cisco Unified CME to provide SRST fallback services for Cisco Unified Communications Manager.
Step 5	**srst dn line-mode** {**dual** | **dual-octo** | **octo** | **single**} **Example:** `Router(config-telephony)# srst dn line-mode dual-octo`	(Optional) Specifies the line mode for ephone-dns in SRST mode on a Cisco Unified CME router. • **dual**—SRST fallback ephone-dns are dual-line ephone-dns. • **dual-octo**—SRST fallback ephone-dns are dual-line or octo-line, depending on the phone type. This keyword is supported in Cisco Unified CME 4.3 and later versions. • **octo**—SRST fallback ephone-dns are octo-line. This keyword is supported in Cisco Unified CME 4.3 and later versions. • **single**—SRST fallback ephone-dns are single-line ephone-dns. Default value. **Note** This command is used only when ephone-dns are learned at the time of fallback. It is ignored when you prebuild ephone-dn configurations.

	Command or Action	Purpose
Step 6	**srst dn template** *template-tag* **Example:** `Router(config-telephony)# srst dn template 3`	(Optional) Specifies an ephone-dn template to be used in SRST mode on a Cisco Unified CME router. The template includes features that were specified when the template was created. See Example for Configuring Templates for Fallback Support: Example, on page 1551. • *template-tag*—identifying number of an existing ephone-dn template. Range is 1 to 15.
Step 7	**srst ephone template** *template-tag* **Example:** `Router(config-telephony)# srst ephone template 5`	(Optional) Specifies an ephone template to be used in SRST mode on a Cisco Unified CME router. • *template-tag*—identifying number of an existing ephone template. Range is 1 to 20.
Step 8	**srst ephone description** *string* **Example:** `Router(config-telephony)# srst ephone description Cisco Unified CME SRST Fallback`	(Optional) Specifies a description to be associated with an ephone learned in SRST mode on a Cisco Unified CME router. • *string*—Description to be associated with an ephone. Maximum string length is 100 characters.
Step 9	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Verify SRST Fallback Mode

Step 1 Use the **show telephony-service all** or the **show running-config** command to verify that SRST fallback mode has been set on this router.

Example:

```
telephony-service
 srst mode auto-provision all
 srst ephone template 5
 srst ephone description srst fallback auto-provision phone : Jul 07 2005 17:45:08
 srst dn template 8
 srst dn line-mode dual
 load 7960-7940 P00305000600
 max-ephones 30
 max-dn 60 preference 0
 ip source-address 10.1.68.78 port 2000
 max-redirect 20
 system message "SRST Mode: Cisco Unified CME'
 keepalive 10
 max-conferences 8 gain -6
 moh welcome.au
```

```
create cnf-files version-stamp Jan 01 2002 00:00:00
```

Step 2 Use the **show telephony-service ephone-dn** command during fallback to review ephone-dn configurations. Learned ephone-dns are noted by a line stating that they were learned during SRST fallback.

Note Learned ephone-dns do not appear in the output for the **show running-config** command if the **none** keyword is used in the **srst mode auto-provision** command.

Example:

```
ephone-dn 1 dual-line
 number 4008
 name 4008
 description 4008
 preference 0 secondary 9
 huntstop
 no huntstop channel
 call-waiting beep
 ephone-dn-template 8
 This DN is learned from srst fallback ephones
```

Step 3 Use the **show telephony-service ephone** command during fallback to review ephone configurations. Learned ephones are noted by a line stating that they were learned during SRST fallback.

Note Learned ephones do not appear in the output for the **show running-config** command if the **none** keyword is used in the **srst mode auto-provision** command.

Example:

```
ephone 1
 mac-address 0112.80B3.9C16
 button 1:1
 multicast-moh
 ephone-template 5
 Always send media packets to this router: No
 Preferred codec: g711ulaw
 user-locale JP
 network-locale US
 Description: "YOUR Description" : Oct 11 2005 09:58:27
 This is a srst fallback phone
```

Prebuilding Cisco Unified CME Phone Configurations

You can optionally create a set of ephone-dns that are preconfigured with extension numbers and some features to provide service during fallback that is similar to the service that is provided during normal operation. Extensions that are not prebuilt are populated with extension numbers and features as they are “learned” by the Cisco Unified CME router in SRST mode at the time of fallback.

Note To avoid incorrect routing when you prebuild ephone-dns for Cisco Unified Communications Manager phones in Cisco Unified CME, use the **preference** command in ephone-dn and voip-dial-peer configuration mode to create a higher preference (0 being the highest) for the voip dial peer than the preference for the prebuilt directory number. For configuration example, see Example for Prebuilding DNs, on page 1552.

See the following procedures to set up a few of the most common features to associate with phones in fallback mode:

- Create Directory Numbers for SCCP Phones, on page 253
- Enable Call Park or Directed Call Park, on page 1089
- Create an Ephone Template, on page 1428
- Create an Ephone-dn Template, on page 1430
- Configure Ephone-Hunt Groups on SCCP Phones, on page 1291

Note Note that the **dial-peer hunt** command must be configured for hunt-selection order of explicit preference to support hunt groups during SRST fallback mode.

Modify Call Pickup for Fallback Support

An especially useful feature for fallback phones is modifying the behavior of the Pickup soft key in Cisco Unified CME to match that of the Pickup soft key in Cisco Unified Communications Manager. To modify the call pickup feature for fallback support, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **no service directed-pickup**
5. **create cnf-files**
6. **reset all**
7. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**no service directed-pickup** **Example:** `Router(telephony)# no service directed-pickup`	(Optional) Disables directed call pickup and changes the behavior of the PickUp soft key so that a user pressing it invokes local group pickup rather than directed call pickup. This behavior is consistent with that of the PickUp soft key in Cisco Unified Communications Manager. **Note** For changes to the service-phone settings to be effective, the Sep*.conf.xml file must be updated with the **create cnf-files** command and the phone units must rebooted with the **reset** command.
Step 5	**create cnf-files** **Example:** `Router(telephony)# create cnf-files`	Builds XML configuration files for Cisco Unified IP phones.
Step 6	**reset all** **Example:** `Router(telephony)# reset all`	Resets all phones.
Step 7	**exit** **Example:** `Router(telephony)# exit`	Exits dial-peer configuration mode.

Configuration Examples for SRST Fallback Mode

Example for Enabling SRST Mode

The following example enables SRST mode on the Cisco Unified CME router. It specifies that learned fallback ephone-dns should be created in dual-line mode and use ephone-dn template 3 for their configuration parameters. Learned ephones will use the parameters in ephone template 5 and a description will be associated with the phones.

```
telephony-service
 max-ephones 30
 max-dn 60 preference 0
 srst mode auto-provision all
 srst dn line-mode dual
 srst dn template 3
```

```
 srst ephone description srst fallback auto-provision phone
 srst ephone template 5
.
.
.
```

The following excerpt from the **show running-config** command displays the configuration of ephone 1, which was learned during fallback; the description is stamped with the date and time that the **show running-config** command was used. The configuration of ephone 2, which was prebuilt rather than learned, is shown for comparison.

```
ephone 1
 description srst fallback auto-provision phone : Jul 07 2005 17:45:08
 ephone-template 5
 mac-address 100A.7052.2AAE
 button 1:1 2:2

ephone 2
 mac-address 1002.CD64.A24A
 type 7960
 button  1:3
```

The following excerpt from the **show running-config** command displays the configuration of ephone-dn 1 through ephone-dn 3. All three ephones are learned ephone-dns that are configured in dual-line mode and use ephone-dn template 5, as specified in the telephony-service configuration mode commands.

```
ephone-dn  1 dual-line
 number 7001
 description 7001
 name 7001
 ephone-dn-template 5
 This DN is learned from srst fallback ephones
!
!
ephone-dn  2 dual-line
 number 4005
 name 4005
 ephone-dn-template 5
 This DN is learned from srst fallback ephones
!
!
ephone-dn  3 dual-line
 number 4002
 label 4002
 name 4002
 ephone-dn-template 5
 This DN is learned from srst fallback ephones
```

Example for Provisioning Directory Numbers for Fallback Support

The following example sets up five ephone-dns and two call-park slots that are used for fallback phones.

```
ephone-dn 1
 number 1101
 name Register 1

ephone-dn 2
 number 1102
 name Register 2

ephone-dn 3
 number 1103
 name Register 3

ephone-dn 4
 number 1104
```

```
 name Register 4

ephone-dn 5
 number 1105
 name Register 5

ephone-dn 21
 number 1121
 name Park Slot 1
 park-slot timeout 60 limit 3 recall alternate 1100

ephone-dn 22
 number 1122
 name Park Slot 2
 park-slot timeout 60 limit 3 recall alternate 1100
```

Example for Configuring Templates for Fallback Support: Example

The following example creates ephone-dn template 3 and ephone template 5 that will be used with the SRST fallback support using Cisco Unified CME feature. Ephone-dn template 3 adds the fallback phones to pickup group 24 and specifies call forwarding for busy and no-answer conditions to extension 1100. Ephone template 5 defines two fastdial numbers that will appear as menu entries displayed from the **Directories** > **Local Services** > **Personal Speed Dials** option on the fallback phones, and also specifies the softkey layouts for the fallback phones.

```
ephone-dn-template 3
 pickup-group 24
 call-forward busy 1100
 call-forward noan 1100 timeout 45

ephone-template 5
 fastdial 1 1101 name Front Register
 fastdial 2 918005550111 Headquarters
 softkeys idle Newcall Cfwdall Pickup
 softkeys seized Endcall Cfwdall Pickup
 softkeys alerting Endcall
 softkeys connected Endcall Hold Park Trnsfer
```

Example for Enabling Hunt Groups for Fallback Support

The following example configures the dial peers to hunt in the following order: (1) explicit preference, (2) longest match in phone number, and (3) random selection. The **dial-peer hunt** command must be configured for hunt-selection order of explicit preference to support hunt groups during SRST fallback mode.

```
dial-peer hunt 2
```

The following example creates a peer hunt group with the pilot number 1111.

```
ephone-hunt 3 peer
 pilot 1111
 list 1101, 1102, 1103
 hops 3
 timeout 25
 final 1100
```

Example for Modifying Call Pickup for Fallback Support

The following example changes the behavior of the Pickup soft key to be like the one in Cisco Unified Communications Manager.

```
telephony-service
 no service directed-pickup
 create cnf-files
```

Example for Prebuilding DNs

In the following partial example, the **preference** command in ephone-dn and voip-dial-peer configuration mode is configured to create a voip dial peer with a higher preference (0) than the preference (1) of the manually-configured directory number (ephone-dn 1).

```
dial-peer voice 1002
  voip destination-pattern 1019
  .
  .
  .
  preference 0 <<=====This dial peer has precedence and will match first.

ephone-dn 1
  number 1019
  preference 1 <<======Configure lower preference for prebuilt DN.
```

Feature Information for SRST Fallback Mode

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

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

Table 118: Feature Information for SRST Fallback Mode

Feature Name	Cisco Unified CME Version	Feature Information
Octo-Line Directory Numbers	4.3	Support for octo-line directory numbers was added.
SRST Fallback Support Using Cisco Unified CME	4.0	SRST fallback support using Cisco Unified CME was introduced.

CHAPTER 52

VRF Support

Virtual Route Forwarding (VRF) divides a physical router into multiple logical routers, each having its own set of interfaces and routing and forwarding tables. VRF support in voice networks can be used to split Cisco Unified Communications Manager Express (Cisco Unified CME) into multiple virtual systems for SIP and SCCP endpoints and TAPI-based client applications and softphones on your PC.

Prerequisites for Configuring VRF Support

- For Multi-VRF support on SIP phones, Cisco Unified CME version has to be 10.5 and later.
- For Multi-VRF support on SCCP phones, Cisco Unified CME 7.0(1) or a later version must be configured on the Cisco router.
- VRF-Aware H.323 and SIP must be configured on the Cisco Unified CME router, including the following:
    - Up to five VRFs must be configured on the Cisco Unified CME router by using the **ip vrf** command. For configuration information, see VRF-Aware H.323 and SIP for Voice Gateways.
    - One of the groups must be designated as a global voice VRF (SIP Trunk) by using the**voice vrf** command. For configuration information, see VRF-Aware H.323 and SIP for Voice Gateways.

      Example:

      ```
      voice vrf voice-vrf
      ip vrf data-vrf1
       rd 801:1
       route-target export 801:1
       route-target import 1000:1
      !
      ip vrf data-vrf2
      ```

```
 rd 802:1
 route-target export 802:1
 route-target import 1000:1
!
ip vrf voice-vrf
 rd 1000:1
 route-target export 1000:1
 route-target import 801:1
 route-target import 802:1
!
```

- Interfaces on the router must be configured for the VRFs by using the **ip vrf forwarding** command.

Note Only global voice VRF is supported for SIP trunk.

Example:

```
interface GigabitEthernet0/0.301
 encapsulation dot1Q 301
 ip vrf forwarding data-vrf1
 ip address 10.1.10.1 255.255.255.0
!
interface GigabitEthernet0/0.302
 encapsulation dot1Q 302
 ip vrf forwarding data-vrf1
 ip address 10.2.10.1 255.255.255.0
!
interface GigabitEthernet0/0.303
 encapsulation dot1Q 303
 ip vrf forwarding voice-vrf
 ip address 10.3.10.1 255.255.255.0
```

- VRFs must be mapped to IP addresses using DHCP. For configuration information, see DHCP Service, on page 122.

Example:

```
!<=== no ip dhcp command required only if “ip vrf forward” is specified under ip dhcp
no ip dhcp use vrf connected pool===>
!<=== Associate subnets with VRFs. Overlapping IP addresses are NOT supported.===>
ip dhcp pool vcme1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   option 150 ip 10.1.10.1
   class vcme1
      address range 10.1.10.10 10.1.10.250
!
ip dhcp pool vcme2
   network 10.2.10.0 255.255.255.0
   default-router 10.2.10.1
   option 150 ip 10.2.10.1
   class vcme2
      address range 10.2.10.10 10.2.10.250
```

For more configuration examples, see Example for Mapping IP Address Ranges to VRF Using DHCP, on page 1565.

- Dial peers for H323 and SIP trucks must be routed through the global voice VRF.

Note Dial peers are global resources belonging to the voice VRF and shared with and accessible from any VRF. There is no need to configure a dial peer for each individual VRF.

Restrictions for Configuring VRF Support

- Multi-VRF is not supported on Cisco 4000 Series Integrated Services Routers for Unified CME.
- For SIP phones in Cisco Unified CME: SIP proxy and registrar must be in the same VRF.
- IP-address overlap between VRFs is not supported.
- Cross-VRF video is not supported.
- The following call types are not supported for a voice VRF:
    - IP-to-IP gateway and gatekeeper configured on the same router.
    - IP-to-IP gateway with a VRF configured on one call leg and not on another call leg.
    - IP-to-IP gateway with one VRF configured for the H.323 call leg and a different VRF configured for the SIP call leg.
    - For H.323 calls, only TCP is supported. H.323 UDP signaling is not supported. SIP calls support both TCP and UDP signaling.
- The following features are not supported by on a VRF:
    - Call-fallback and RSVP features.
    - H.323 Annex E calls.
    - AAA and DNS components in voice-capable access routers. These routers communicate with AAA and DNS using the default routing table.
- If a global voice VRF is not configured, signaling and media packets are sent using the default routing table.
- Only the global voice VRF is supported for SIP trunk.
- Cisco Unity Express on the Cisco Unified CME router must belong to the global voice VRF.

Note Telnet is used to access Cisco Unity Express on the global voice VRF because the Service-Engine Service-Engine 1/0 session command is for non-VRF aware Cisco Unified CME only. To access the Cisco Unity Express module for defining voice-mail users on global voice VRF, telnet through the global voice VRF. For example: telnet 10.10.10.5 2066 /vrf vrf. For more information, see the "*Installing Cisco Unity Express Software*" chapter in the appropriate Cisco Unity Express Administrator Guide for Cisco Unified CME.

Information About VRF Support

VRF-Aware Cisco Unified CME

VRF implementations enable you to consolidate voice communication into one logically-partitioned network to separate voice and data communication on a converged multimedia network.

VRF-Aware Cisco Unified CME for SCCP Phones

In Cisco Unified CME 7.0(1) and later versions, VRF in voice networks can be used to share a Cisco Unified CME among multiple closed-users groups with different requirements. The actual call processing rules can be applied by voice on a per VRF basis. A virtual Cisco Unified CME on each VRF is a collection of phones in VRF groups that register in Cisco Unified CME through the VRF. All SCCP and SIP phones connected to Cisco Unified CME register through the global voice VRF. TAPI-based client applications and softphones on a PC must register through a data VRF and can communicate with phones on the voice VRF.

VRF Support on Cisco Unified CME provides the following enhancements to the VRF-Aware H.323 and SIP for Voice Gateways feature:

- Line side support for up to 5 VRFs.
- Interworks with the global voice VRF on an H323 or SIP Trunk.
- Line side VRF can be a global voice VRF.
- VRFs are assigned on a per-phone level.
- Support for cross-VRF shared-lines.

For configuration information, see Configure VRF Support, on page 1556.

Multi-VRF Support on Cisco Unified CME for SIP Phones

The Multi-VRF support on Cisco Unified CME for SIP Phones, provides the following enhancements:

- Up to 5 VRF groups can be configured on SIP line side under voice register global.
- Under voice register pool, we can configure a VRF group to which the phone is associated with.
- All SIP signaling and media traffic between CME and the phones would be routed on the specified VRF.

Configure VRF Support

Create VRF Groups for SCCP Phones

To configure up to five VRF groups for users and phones in Cisco Unified CME, perform the following steps for each group to be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **group** *group-tag* [**vrf** vrf*name*]
5. **ip source-address** *ip-address* [**port** *port*]
6. **url** {**authentication** | **directories** |**idle** | **information** | **messages** | **proxy-server** |**services**} *url*
7. **service phone webAccess 0**
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**group** *group-tag* [**vrf** vrf*name*] **Example:** `Router(config-telephony)# group 1`	Creates a VRF group for Cisco Unified CME users and phones. • *group-tag*—Unique identifier for VRF group being configured. Range: 1 to 5. • (Optional) **vrf** *vrfname*—Name of previously configured VRF to which this group is associated. • By default, VRF groups are associated with a global voice VRF unless otherwise specified by using the **vrf***vrfname* keyword and argument combination.
Step 5	**ip source-address** *ip-address* [**port** *port*] **Example:** `Router(conf-tele-group)# ip source-address 10.1.10.1 port 2000`	Associates VRF group with Cisco Unified CME. • *ip address* and **port** through which Cisco Unified IP phones communicate with Cisco Unified CME.

	Command or Action	Purpose
Step 6	**url** {**authentication** | **directories** |**idle** | **information** | **messages** | **proxy-server** |**services**} *url* **Example:** `Router(conf-tele-group)# url directories http://10.1.10.1/localdirectory`	Provisions uniform resource locators (URLs) for Cisco Unified IP phones connected to Cisco Unified CME.
Step 7	**service phone webAccess 0** **Example:** `Router(conf-tele-group)# service phone webAccess 0`	Enables webAccess for IP phones. This is required for 9.x firmware, since the web server is disabled by default. 8.x firmware and lower had the web server enabled by default.
Step 8	**end** **Example:** `Router(conf-tele-group)# end`	Returns to privileged EXEC mode.

Examples

The following partial output from the **show running-config** commands shows how to define three VRF groups for Cisco Unified CME. Group 1 is on the global voice VRF and the other two groups are on data VRFs.

```
telephony-service
 sdspfarm conference mute-on # mute-off #
 sdspfarm units 4
 sdspfarm transcode sessions 10
 sdspfarm tag 1 xcode101
 sdspfarm tag 2 conf103
 group  1
  ip source-address 10.1.10.1 port 2000
  url directories http://10.1.10.1/localdirectory
 !
 group  2 vrf data-vrf1
  ip source-address 10.2.10.1 port 2000
 !
 group  3 vrf data-vrf2
  ip source-address 10.3.10.1 port 2000
```

Create VRF Groups for SIP Phones

In Cisco Unified CME 10.5 release the VRF support for SIP phones is added. Up to five VRF groups can be configured on SIP line side under voice register global. Under voice register pool, we can configure VRF group to which the phone is associated with. To configure VRF support, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **group** *group-tag* [**vrf** *vrfname*]
5. **source-address** *ip-address*
6. **url** {**authentication** | **directory** | **service**} *url*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice register global** **Example:** `Router(config)# voice register global`	Enters voice register global configuration mode.
Step 4	**group** *group-tag* [**vrf** *vrfname*] **Example:** `Router(config-register-global)# group 1`	Creates a VRF group for Cisco Unified CME users and phones. • *group-tag*—Unique identifier for VRF group being configured. Range: 1 to 5. • (Optional) **vrf** *vrfname*—Name of previously configured VRF to which this group is associated. • By default, this group is not associated with any VRF unless otherwise specified by using the **vrf** *vrfname* keyword and argument combination. • Defines unique identifiers group between 1 to 5, which can then be applied on individual pools. **Note** Use the shutdown command to temporarily shutdown the group without effecting the other groups. Use the no form of the command to enable the group. • The default behavior is no shut.
Step 5	**source-address** *ip-address*	Associates VRF group with Cisco Unified CME.

	Command or Action	Purpose
	Example: `Router(config-voice-register-group)# source-address 10.1.10.1`	• *ip address* through which Cisco Unified IP phones communicate with Cisco Unified CME.
Step 6	**url** {**authentication** | **directory** | **service**} *url* **Example:** `Router(config-voice-register-group)# url directory http://10.1.10.1/localdirectory`	Provisions uniform resource locators (URLs) for Cisco Unified IP phones connected to Cisco Unified CME.
Step 7	**exit** **Example:** `Router(config-voice-register-group)# exit`	Exits to privileged EXEC mode.

Examples

The following sample output displays how to configure SIP CME support for VRF by provisioning its source address under a group:

```
voice register global or
voice register dn
or
voice register pool
 mode  cme
 max-dn 100
 max-pool 100

 group 1 vrf voice-vrf1
  source-address 8.0.0.1
```

Add Cisco Unified CME SCCP Phones to a VRF Group

To add an SCCP Cisco Unified IP phone, TAPI-based client, or softphone in Cisco Unified CME to a VRF group, perform the following steps for each phone to be added.

Restriction

- All SCCP phones in Cisco Unified CME must register through the global voice VRF and must be added to the VRF group on the global voice VRF only.
- Analog phones connected to FXS ports on a IOS gateway must register through the global voice VRF and must be added to the VRF group on the global voice VRF only.
- TAPI-based client applications and softphones on a PC must register through the data VRF and must be added to a VRF group on a data VRF only.
- VRF groups do not support identical IP addresses or shared lines.

Before You Begin

- All ephone configurations to be included in a VRF group must be already configured in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **description** *string*
5. **mac-address** [*mac-address*]
6. **group phone** *group-tag* [**tapi** *group-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	**ephone** *phone-tag* **Example:** `Router(config)# ephone 11`	Enters ephone configuration mode for a Cisco Unified IP phone.

	Command or Action	Purpose
Step 4	**description** *string* **Example:** `Router(config-ephone)# description cme-2801 srst`	(Optional) Includes descriptive text about the interface.
Step 5	**mac-address** [*mac-address*] **Example:** `Router(config-ephone)# mac-address 0012.8055.d2EE`	Associates the MAC address of a Cisco Unified IP phone with an ephone configuration.
Step 6	**group phone** *group-tag* [**tapi** *group-tag*] **Example:** `Router(config-ephone)# group phone 1`	Adds a phone, TAPI-based client, or softphone to a VRF group. • *group-tag*—Unique identifier for VRF group that was previously configured by using the **group** command in telephony-service configuration mode. Range: 1 to 5. • This command can also be configured in ephone-template configuration mode and applied to one or more phones. The ephone configuration has priority over the ephone-template configuration.
Step 7	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Examples

The following example shows how to add phones to VRF groups. Phones 1 and 3 are in VRF group 1 on the global voice VRF. Phone 1 TAPI client and softphone 3 are in group 1 on the data-vrf2. Phone 3 TAPI client and softphone 4 are in group 3 on data-vrf 2.

```
telephony-service
 sdspfarm conference mute-on # mute-off #
 sdspfarm units 4
 sdspfarm transcode sessions 10
 sdspfarm tag 1 xcode101
 sdspfarm tag 2 conf103
 group  1 vrf voice-vrf
  ip source-address 10.1.10.1 port 2000
  url directories http://10.1.10.1/localdirectory
 !
 group  2 vrf data-vrf1
  ip source-address 10.2.10.1 port 2000
 !
group  3 vrf data-vrf2
  ip source-address 10.3.10.1 port 2000
 !
.
.
ephone-template 1
```

```
 group phone 1 tapi 2
ephone-template 2
 group phone 2
...
ephone 1
 ephone-template 1
ephone 2
 ephone-template 2
ephone 3
 group phone 1 tapi 3
ephone 4
 group phone 3
ephone  201
 group phone 1
 type anl
```

Add Cisco Unified CME SIP Phones to a VRF Group

To add an SIP Cisco Unified IP phone, or softphone in Cisco Unified CME to a VRF group, perform the following steps for each phone to be added.

Before You Begin

- All voice register pool configurations to be included in a VRF group must be already configured in Cisco Unified CME. For configuration information, see Configure Phones to Make Basic Call, on page 315.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **id mac** [*mac-address*]
5. **group** *group-tag*
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.

	Command or Action	Purpose
Step 3	**voice register pool** *pool-tag* **Example:** `Router(config-register-pool)# group`	Enters voice reigster pool configuration mode for a Cisco Unified IP phone.
Step 4	**id mac** [*mac-address*] **Example:** `Router(config-regoster-pool)# id mac 0012.8055.d2EE`	Associates the MAC address of a Cisco Unified IP phone with an voice register pool configuration.
Step 5	**group** *group-tag* **Example:** `Router(config-register pool)# group 1`	Adds a phone, or softphone to a VRF group. • *group-tag*—Unique identifier for VRF group that was previously configured by using the **group** command in voice register global configuration mode. Range: 1 to 5.
Step 6	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Examples

The following example shows how to add SIP phones to VRF groups.

```
voice register global
   mode  cme
   max-dn 100
   max-pool 100
   authenticate realm ccmsipline
   voicemail 24001
   phone-mode phone-only
   tftp-path flash:
   create profile sync 0000443960010126
   conference hardware
   group 1 vrf voice-vrf1
    source-address 8.0.0.1
   !
   group 2 vrf data-vrf1
    url authentication http://7.0.0.1/CCMCIP/authenticate.asp
    source-address 7.0.0.1
   !
   group 3 vrf data-vrf1
    source-address 10.104.45.142
   !
   group 4 vrf voice-vrf1
    source-address 9.42.29.101
   !
  !
  voice register pool  1
   id mac A40C.C395.7B5C
   session-transport tcp
   type 9971
   number 1 dn 1
   group 1
   template 1
```

```
   dtmf-relay rtp-nte
   username 14001 password 14001
   codec g711ulaw
   paging-dn 99
  !
```

Configuration Examples for Configuring VRF Support

Example for Mapping IP Address Ranges to VRF Using DHCP

Note Duplicate IP addresses, with or without specifying a VRF, are not supported in Cisco Unified CME 7.0(1).

There are three ways to assign DHCP addresses: global address allocation; VRF pool; or individual host

With a global address allocation scheme, you must use the **no ip dhcp use vrf connected** command.

```
no ip dhcp use vrf connected
!
ip dhcp pool vcme1
   network 209.165.201.10 255.255.255.224
   option 150 ip 209.165.201.9
   default-router 209.165.201.9
   class vcme1
      address range 209.165.201.1 209.165.201.30
!
```

The following example shows how to assign addresses from VRF pool vcme1.

```
ip dhcp use vrf connected
!
ip dhcp pool vcme1
   vrf data-vrf1
   network 209.165.201.10 255.255.255.224
   option 150 ip 209.165.201.9
   default-router 209.165.201.9
   class vcme1
      address range 209.165.201.1 209.165.201.30
!
```

The following example show how to assign an address by an individual host. You must replace the first two hexadecimal digits of a host MAC address with **01**.

```
ip dhcp pool phone3
   host 209.165.201.15 255.255.255.224
   client-identifier 0100.0ed7.4ce6.3d
   default-router 209.165.201.11
   option 150 ip 209.165.201.11
!
```

Example for Configuring VRF-Aware Hardware Conferencing

Hardware Conferencing with Internal DSP Farm

- The internal DSPFarm must be registered through a local loopback interface.

- The loopback allows Cisco Unified CME to access the media path in global routing table.

The boldface commands in the following configuration example show that the signaling and media paths are accessed through the global routing table and the loopback interface is in default routing table.

```
interface Loopback5
  ip address 12.5.10.1 255.255.255.255
 !
 sccp local Loopback5
 sccp ccm 12.5.10.1 identifier 2 version 4.1
 sccp
 !
 sccp ccm group 2
  bind interface Loopback5
  associate ccm 2 priority 1
  associate profile 103 register conf103
  associate profile 101 register xcode101
 !
 telephony-service
  sdspfarm conference mute-on # mute-off #
  sdspfarm units 4
  sdspfarm transcode sessions 10
  sdspfarm tag 1 xcode101
  sdspfarm tag 2 conf103
  group  1 vrf vrf1
  ip source-address 10.1.10.1 port 2000
 !
  group  2 vrf vrf2
   ip source-address 10.2.10.1 port 2000
 !
 group  3 vrf vrf3
   ip source-address 10.3.10.1 port 2000
 !
 group  4 vrf vrf4
   ip source-address 10.4.10.1 port 2000
 !
  group  5
   ip source-address 12.5.10.1 port 2000
 !
 conference hardware
 max-ephones 240
 max-dn 480
 voicemail 7710
 max-conferences 8 gain -6
```

Hardware Conferencing with External DSP Farm

- Configure DSP farm as usual on a Cisco router.
- The external DSP farm must be registered to Cisco Unified CME through the interface or subinterface assigned to the global voice VRF. Make sure the connection path is coming in through the voice VRF.
- The router on which the external DSP farm is configured does not have to be VRF-aware.

For information about configuring DSP Farms, see Configure Transcoding Resources, on page 479.

Example for Configuring Cisco Unity Express on Global Voice VRF

```
voice vrf vrf2
 ip vrf data-vrf2
 rd 100:2
 route-target export 100:2
```

```
 route-target import 100:2
!
Interface loop back 0
ip vrf forwarding data-vrf2
Ip address 21.10.10.2
!<==The following config puts CUE in the voice vrf. Service-engine interface and
service-module must have an IP address.===>
!
interface Service-Engine1/0
 ip vrf forwarding voice-vrf3 ip address 21.10.10.5 255.255.255.0
 service-module ip address 21.10.10.6 255.255.255.0
 service-module ip default-gateway 21.10.10.2!
 ip route 21.10.10.6 255.255.255.255 Service-Engine1/0
…
line 66
no activation-character
```

Hardware Conferencing with Internal DSP Farm

- The internal DSPFarm must be registered through a local loopback interface.
- The loopback allows Cisco Unified CME to access the media path in global routing table.

The boldface commands in the following configuration example show that the signaling and media paths are accessed through the global routing table and the loopback interface is in default routing table.

```
interface Loopback5
 ip address 12.5.10.1 255.255.255.255
!
sccp local Loopback5
sccp ccm 12.5.10.1 identifier 2 version 4.1
sccp
!
sccp ccm group 2
 bind interface Loopback5
 associate ccm 2 priority 1
 associate profile 103 register conf103
 associate profile 101 register xcode101
!
telephony-service
 sdspfarm conference mute-on # mute-off #
 sdspfarm units 4
 sdspfarm transcode sessions 10
 sdspfarm tag 1 xcode101
 sdspfarm tag 2 conf103
 group  1 vrf vrf1
  ip source-address 10.1.10.1 port 2000
!
 group  2 vrf vrf2
  ip source-address 10.2.10.1 port 2000
!
group  3 vrf vrf3
  ip source-address 10.3.10.1 port 2000
!
group  4 vrf vrf4
  ip source-address 10.4.10.1 port 2000
!
 group  5
 ip source-address 12.5.10.1 port 2000
!
conference hardware
max-ephones 240
max-dn 480
voicemail 7710
max-conferences 8 gain -6
```

Hardware Conferencing with External DSP Farm

- Configure DSP farm as usual on a Cisco router.
- The external DSP farm must be registered to Cisco Unified CME through the interface or subinterface assigned to the global voice VRF. Make sure the connection path is coming in through the voice VRF.
- The router on which the external DSP farm is configured does not have to be VRF-aware.

For information about configuring DSP Farms, see Configure Transcoding Resources, on page 479.

Example for Configuring Multi- VRF Support for Cisco Unified CME SIP Phones

The following sample output displays CME configuration which enables the user to accept registrations from multiple VRFs.

```
voice register global
 mode  cme
 max-dn 100
 max-pool 100
 authenticate realm ccmsipline
 voicemail 24001
 phone-mode phone-only
 tftp-path flash:
 create profile sync 0000443960010126
 conference hardware
 group 1 vrf voice-vrf1
  source-address 8.0.0.1
 !
 group 2 vrf data-vrf1
  url authentication http://7.0.0.1/CCMCIP/authenticate.asp
  source-address 7.0.0.1
 !
 group 3 vrf data-vrf1
  source-address 10.104.45.142
 !
 group 4 vrf voice-vrf1
  source-address 9.42.29.101
 !
!
voice register dn  1
 number 14001
 name voicevrf-ph1
!
voice register dn  2
 number 14002
 allow watch
 name datavrf-ph1
!
voice register dn  3
 number 14003
 allow watch
 name voicevrf-ph2
!
voice register dn  4
 voice-hunt-groups login
 number 14004
 name Jabber-Win
!
voice register dn  5
 number 14005
 name Jabber-Android
!
voice register dn  6
 number 14006
 allow watch
 mobility
 snr 24001 delay 5 timeout 50
!
```

```
voice register dn  7
 number 14007
 name voicevrf-7841
!
voice register dn  8
 number 14008
 name jabbed-android-2
!
voice register dn  10
 number 14010
 allow watch
 name intervrf-shared-line
 shared-line max-calls 8
!
voice register dn  11
 number 14011
 shared-line
!
voice register dn  12
 number 15002
 name em-logged-in
!
voice register dn  21
 number 1101
 name CME1-Phone1
!
voice register dn  22
 number 1102
 name CME1-Phone2
!
voice register template  1
 softkeys idle  Newcall Pickup Redial Cfwdall DND
 softkeys ringIn  Answer DND iDivert
 softkeys connected  Endcall Hold Mobility iDivert Park
!
voice register pool  1
 id mac A40C.C395.7B5C
 session-transport tcp
 type 9971
 number 1 dn 1
 group 1
 template 1
 dtmf-relay rtp-nte
 username 14001 password 14001
 codec g711ulaw
 paging-dn 99
!
voice register pool  2
 fastdial 1 14003 name voice-vrf1-ph1
 id mac ACA0.16FC.9742
 type 9971
 number 1 dn 2
 number 2 dn 10
 group 2
 template 1
 presence call-list
 dtmf-relay rtp-nte
 codec g711ulaw
 paging-dn 99
 blf-speed-dial 1 13001 label "13001"
 blf-speed-dial 2 14006 label "14006"
!
voice register pool  3
 fastdial 1 14002 name datavrf,ph1
 id mac 2893.FEA3.2557
 type 9951
 number 1 dn 3
 number 2 dn 10
 group 1
 template 1
 dtmf-relay rtp-nte
 username 14003 password 14003
 codec g711ulaw
```

```
 blf-speed-dial 1 14002 label "14002"
 blf-speed-dial 2 14006 label "14006"
 blf-speed-dial 3 13001 label "13001"
!
voice register pool  4
 id device-id-name arunsrin
 type Jabber-CSF-Client
 number 1 dn 4
 group 3
 dtmf-relay rtp-nte
 username arunsrin password cisco
 codec g711ulaw
!
voice register pool  5
 registration-timer max 720 min 660
 id mac 980C.821B.26CD
 session-transport tcp
 type Jabber-Android
 number 1 dn 5
 group 3
 dtmf-relay rtp-nte
 username frodo password cisco
 codec g711ulaw
!
voice register pool  6
 busy-trigger-per-button 40
 id mac 6C41.6A36.900D
 type 7821
 number 1 dn 6
 group 1
 template 1
 presence call-list
 dtmf-relay rtp-nte
 codec g711ulaw
 paging-dn 99
!
voice register pool  7
 busy-trigger-per-button 40
 id mac 6C41.6A36.9110
 session-transport tcp
 type 7841
 number 1 dn 7
 group 2
 dtmf-relay rtp-nte
 codec g711ulaw
 paging-dn 99
!
voice register pool  8
 registration-timer max 720 min 660
 id mac 980C.821A.5D28
 session-transport tcp
 type Jabber-Android
 number 1 dn 8
 group 3
 dtmf-relay rtp-nte
 username pippin password cisco
 codec g711ulaw
!
voice register pool  21
 id mac 1000.1000.1101
 type 7970
 number 1 dn 21
 group 4
 username 1101 password 1101
 codec g711ulaw
!
voice register pool  22
 id mac 1000.1000.1102
 type 7970
 number 1 dn 21
 group 4
 username 1102 password 1102
 codec g711ulaw
```

```
!
voice hunt-group 1 parallel
 phone-display
 final 13002
 list 14001,14002,14003
 timeout 3
 pilot 14999
!
!
voice hunt-group 2 parallel
 final 14001
 list 14004,*,14002
 timeout 5
 pilot 14998
 name test-vhg
!
!
voice logout-profile 1
 pin 1234
 user 14002 password 14002
 number 14002 type normal
 speed-dial 1 13002 label "ephone2"
!
voice user-profile 1
 user me password me
 number 15002 type normal
!
!
!
voice translation-rule 217351
 rule 1 /^24/ /9924\1/
!
!
voice translation-profile 217351
```

Feature Information for VRF Support

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

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

Table 119: Feature Information for Virtual Route Forwarding

Feature Name	Cisco Unified CME Version	Feature Information
VRF Support in Cisco Unified CME	7.0(1)	VRF supports Cisco Unified CME, conferencing, transcoding, and RSVP components. VRF also allows soft phones in data VRF resources to communicate with phones in a VRF voice gateway.

CHAPTER 53

Configure the XML API

This chapter describes the eXtensible Markup Language (XML) Application Programming Interface (API) support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Information About XML API

XML API Definition

An XML API provides an interface to Cisco Unified CME that allows an external network management system (NMS) to configure and monitor Cisco Unified CME operations.

XML API Provision Using IXI

In previous versions of Cisco Unified CME, the XML interface provided configuration and monitoring functions using the HTTP port. The XML interface ran under the HTTP server process, simultaneously parsing incoming XML requests on demand and processing them.

In Cisco Unified CME 4.0 and later versions, the XML interface is provided through the Cisco IOS XML Infrastructure (IXI), in which the parser and transport layers are separated from the application. This modularity provides scalability and enables future XML support to be developed. In Cisco Unified CME 4.0 and later versions, all Cisco Unified CME features have XML support.

XML API for Cisco Unified CME

The eXtensible Markup Language (XML) Application Programming Interface (API) is supported in Cisco Unified Communications Manager Express (Cisco Unified CME) 8.5 and later versions.

Target Audience

This chapter assumes that you have knowledge of a high-level programming language, such as C++, Java, or an equivalent language. You must also have knowledge or experience in the following areas:

- TCP/IP Protocol
- Hypertext Transport Protocol
- Socket programming
- XML

In addition, users of this programming guide must have a firm grasp of XML Schema, which is used to define the AXL requests, responses, and errors. For more information on XML Schema, see XML Schema Part 0: Primer Second Edition.

Prerequisites

- For Cisco Unified CME: XML API must be configured in Cisco Unified CME. For configuration information, see Configure the XML API, on page 1573 of the *Cisco Unified CME Administrator Guide*.

Information on XML API for Cisco Unified CME

The XML API support in Cisco Unified CME provides a mechanism for inserting, retrieving, updating, and removing data from the Cisco router using XML.

Request methods are XML structures that are passed to the XML server in Cisco Unified CME and Cisco Unified SRST applications using HTTP POST. The XML server receives the XML structures and executes the request. If the request completes successfully, then the appropriate XML response is returned.

Note Querying for multiple entities in a single request can fail because of the XML buffer size limitation. Because of this limitation, the application must adjust its granularity to query one entity per request.

Table 120: XML API Methods: Request and Response, on page 1574 lists the request and response methods for the XML API along with the purpose and parameters for each method.

Table 120: XML API Methods: Request and Response

Description	Request	Parameter	Response
System			

Description	Request	Parameter	Response
Execute configuration commands	ISexecCLI	*command*	ISexecCLIResult
Save router configuration to nvram	ISSaveConfig	—	ISSaveConfigResult
SCCP			
Get system status for Cisco Unified CME or Cisco Unified SRST.	ISgetGlobal	—	ISGlobal
Get status of an IP phone	ISgetDevice	Any combination of the following: ISDevID ISDevName ISKeyword: • all • allTag • available	ISDevices
Get configuration of a phone template	ISgetDeviceTemplate	Any combination of the following: ISDevTemplateID ISKeyword: • all • allTag • available	ISDeviceTemplates
Get configuration of an extension	ISgetExtension	Any combination of the following: ISExtID ISExtNumber ISKeyword: • all • allTag • available	ISExtensions

Description	Request	Parameter	Response
Get configuration of an extension template	ISgetExtensionTemplate	Any combination of the following: ISExtTemplateID ISKeyword: • all • allTag • available	ISExtensionTemplates
Get user information	ISgetUser	ISuserID	ISuser
Get user profile information	ISgetuserProfile	Any combination of the following: ISUserProfileID ISuserID ISKeyword: • all • allTag • available	ISUserProfiles
Get configuration for utility directory	ISgetUtilityDirectory	—	ISUtilityDirectory
SIP			
Get system status for a Cisco Unified CME running SIP	ISgetVoiceRegGlobal	—	ISSipGlobal
Get status of an IP phone	ISgetSipDevice	Any combination of the following: ISPoolID ISPoolName ISKeyword: • all • allTag • available	ISSipDevices

Description	Request	Parameter	Response
Get configuration of an extension	ISgetSipExtension	Any combination of the following: ISVoiceRegDNID ISVoiceRegNumber ISKeyword: • all • allTag • available	ISSipExtensions
Get status of a session server	ISgetSessionServer	Any combination of the following: ISSessionServerID ISSessionServerName ISKeyword: • all • allTag • available	ISSessionServers
Get status of voice hunt groups	ISgetVoiceHuntGroup	ISVoiceHuntGroupID ISKeyword: • all • allTag • available	ISVoiceHuntGroups
Get configuration for Presence	ISgetPresenceGlobal	—	ISPresenceGlobal

Examples for XML API Methods

This section contains examples for the following XML API methods:

System

- ISexecCLI
- ISSaveConfig

SCCP IP Phones

- ISgetGlobal
- ISgetDevice
- ISgetDeviceTemplate
- ISgetExtension
- ISgetExtensionTemplate
- ISgetUser
- ISgetUserProfile
- ISgetUtilityDirectory

SIP IP Phones

- ISgetVoiceRegGlobal
- ISgetSipDevice
- ISgetSipExtension
- ISgetSessionServer
- ISgetVoiceHuntGroup
- ISgetPresenceGlobal

ISexecCLI

Use ISexecCLI to execute a list of Cisco IOS commands on the Cisco router. The request must include the CLI parameter with the Cisco IOS command string for each command to be executed.

Request

```
<SOAP-ENV:Envelope>
<SOAP-ENV:Body>
<axl>
<request xsi:type="ISexecCLI">
<ISexecCLI>
<CLI>ephone 4</CLI>
<CLI>mac-address 000D.BC80.EB51</CLI>
<CLI>type 7960</CLI>
<CLI>button  1:1</CLI>
</ISexecCLI>
</request>
</axl>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Response

The value of "0" for ISexecCLIResponse in the following example is the response when the request is completed successfully.

```
<SOAP-ENV:Envelope >
<SOAP-ENV:Body>
<axl >
<response xsi:type="ISexecCLIResponse" >
<ISexecCLIResponse>0</ISexecCLIResponse>
```

```
<ISexecCLIError></ISexecCLIError>
</response>
</axl>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The following example shows the response when the request fails. The value of ISexecCLIResponse identifies which line number in the request failed. Any subsequent commands in the list of commands are not executed. All preceding commands in the list were executed.

```
<SOAP-ENV:Envelope >
<SOAP-ENV:Body>
<axl >
<response xsi:type="ISexecCLIResponse" >
<ISexecCLIResponse>4</ISexecCLIResponse>
<ISexecCLIError> invalid input dn parameter for button 1</ISexecCLIError>
</response>
</axl>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

ISSaveConfig

Use ISSaveConfig to save the running configuration on a router to the startup configuration on the same router.

Request

```
<request>
<ISSaveConfig />
</request>
```

Response

The following example shows that the ISSaveConfig request was successfully completed.

```
<response xsi:type=" ISSaveConfig">
<ISSaveConfigResult>success</ISSaveConfigResult>
</request>
```

The following example shows the response when the request fails.

```
<response xsi:type=" ISSaveConfig">
<ISSaveConfigResult>fail</ISSaveConfigResult>
</request>
```

The following example shows that response when the request is delayed, typically because there is another terminal session connected to Cisco Unified CME. The running configuration will be saved later by a background process after all other terminal sessions are disconnected.

```
<response xsi:type=" ISSaveConfig">
<ISSaveConfigResult>delay</ISSaveConfigResult>
</request>
```

ISgetGlobal

Use ISgetGlobal to retrieve system configuration and status information for the Cisco Unified CME system.

Request

```
<request xsi:type="ISgetGlobal”>
<ISgetGlobal></ISgetGlobal>
</request>
```

Response


```
<response>
<ISGlobal>
<ISAddress>10.4.188.90</ISAddress>
<ISMode>ITS</ISMode>
<ISVersion>7.2</ISVersion>
<ISDeviceRegistered>0</ISDeviceRegistered>
<ISPeakDeviceRegistered>1</ISPeakDeviceRegistered>
<ISPeakDeviceRegisteredTime>9470</ISPeakDeviceRegisteredTime>
<ISKeepAliveInterval>30</ISKeepAliveInterval>
<ISConfiguredDevice>32</ISConfiguredDevice>
<ISConfiguredExtension>74</ISConfiguredExtension>
<ISServiceEngine>0.0.0.0</ISServiceEngine>
<ISName>ngm-2800</ISName>
<ISPortNumber>2000</ISPortNumber>
<ISMaxConference>8</ISMaxConference>
<ISMaxRedirect>10</ISMaxRedirect>
<ISMaxEphone>48</ISMaxEphone>
<ISMaxDN>180</ISMaxDN>
<ISVoiceMail>6050</ISVoiceMail>
<ISUrlServices>
<ISUrlService>
<ISUrlType>EPHONE_URL_INFO</ISUrlType>
<ISUrlLink>http://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
<ISUrlService>
<ISUrlType>EPHONE_URL_DIRECTOREIES</ISUrlType>
<ISUrlLink>http://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
<ISUrlService>
<ISUrlType>EPHONE_URL_MESSAGES</ISUrlType>
<ISUrlLink>http://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
<ISUrlService>
<ISUrlType>EPHONE_URL_SERVICES</ISUrlType>
<ISUrlLink>http://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
<ISUrlService>
<ISUrlType>EPHONE_URL_PROXYSERV</ISUrlType>
<ISUrlLink>http://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
<ISUrlService>
<ISUrlType>EPHONE_URL_IDLE</ISUrlType>
<ISUrlLink>ttp://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
<ISUrlService>
<ISUrlType>EPHONE_URL_AUTH</ISUrlType>
<ISUrlLink>http://1.4.188.101/localdir</ISUrlLink>
</ISUrlService>
</ISUrlServices>
<global-after-hours>
<block_list>
<block_item>
<pattern_id>1</pattern_id>
<blocking_pattern>1234</blocking_pattern>
<blocking_option />
</block_item>
<block_item>
<pattern_id>2</pattern_id>
<blocking_pattern>2345</blocking_pattern>
<blocking_option>7-24</blocking_option>
</block_item>
</block_list>
<date_list>
<date_item>
<month>Nov</month>
<day_of_month>12</day_of_month>
<start_time>12:00</start_time>
<stop_time>13:00</stop_time>
</date_item>
</date_list>
```

```
<day_list>
<day_item>
<day_of_week>Mon</day_of_week>
<start_time>12:00</start_time>
<stop_time>13:00</stop_time>
</day_item>
</day_list>
<after-hours_login>
<http>true</http>
</after-hours_login>
<override-code>2222</override-code>
<pstn-prefix_list>
<pstn-prefix_item>
<index>1</index>
<pstn-prefix>22</pstn-prefix>
</pstn-prefix_item>
</pstn-prefix_list>
</global-after-hours>
<application_name>calling</application_name>
<auth_credential_list>
<credential_item>
<index>1</index>
<user>test</user>
<password>test</password>
</credential_item>
</auth_credential_list>
<auto>
<assign_list>
<assign_item>
<group_id>1</group_id>
<start_tag>70</start_tag>
<stop_tag>93</stop_tag>
<type>anl</type>
<cfw />
<timeout>0</timeout>
</assign_item>
<assign_item>
<group_id>2</group_id>
<start_tag>1</start_tag>
<stop_tag>20</stop_tag>
<cfw>1234</cfw>
<timeout>80</timeout>
</assign_item>
</assign_list>
</auto>
<auto-reg-ephone>true</auto-reg-ephone>
<bulk-speed-dial_list>
<bulk-speed-dial_item>
<list>1</list>
<url />
</bulk-speed-dial_item>
</bulk-speed-dial_list>
<prefix>123<prefix>
<global-call-forward>
<pattern_list>
<pattern_item>
<index>2</index>
<pattern>.T</pattern>
</pattern_item>
</pattern_list>
<callfwd_system>
<redirecting-expanded>false</redirecting-expanded>
</callfwd_system>
</global-call-forward>
<call-park>
<select>
<no-auto-match>true</no-auto-match>
</select>
<application_system>true</application_system>
<redirect_system>true</redirect_system>
</call-park>
<caller-id>
<block_code>*1</block_code>
```

```
<name-only>true</name-only>
</caller-id>
<calling-number>
<initiator>true</initiator>
<local>false</local>
<secondary>false</secondary>
</calling-number>
<cnf-file>
<location>
<TFTP>flash:/its/</TFTP>
<flash>true</flash>
</location>
<option>perphonetype</option>
</cnf-file>
<default_codec>Unknown</default_codec>
<conference>
<hardware>true</hardware>
</conference>
<date-format>mm-dd-yy</date-format>
<device-security-mode>none</device-security-mode>
<dialplan-pattern_list>
<dialplan-pattern_item>
<index>1</index>
<pattern>1234</pattern>
<extension-length>4</extension-length>
<extension-pattern />
<demote>false</demote>
<no-reg>false</no-reg>
</dialplan-pattern_item>
<dialplan-pattern_item>
<index>2</index>
<pattern>1233</pattern>
<extension-length>4</extension-length>
<extension-pattern />
<demote>true</demote>
<no-reg>false</no-reg>
</dialplan-pattern_item>
<dialplan-pattern_item>
<index>3</index>
<pattern>1232</pattern>
<extension-length>4</extension-length>
<extension-pattern>1111</extension-pattern>
<demote>false</demote>
<no-reg>false</no-reg>
</dialplan-pattern_item>
<dialplan-pattern_item>
<index>4</index>
<pattern>1231</pattern>
<extension-length>4</extension-length>
<extension-pattern />
<demote>false</demote>
<no-reg>true</no-reg>
</dialplan-pattern_item>
</dialplan-pattern_list>
<directory>
<entry_list>
<entry_item>
<tag>1</tag>
<number>1234</number>
<name>directory</name>
</entry_item>
</entry_list>
<option>last-name-first</option>
</directory>
<dn-webedit>false</dn-webedit>
<em>
<external>true</external>
<keep-history>true</keep-history>
<logout>12:00 00:-1 -1:-1</logout>
</em>
<ephone-reg>true</ephone-reg>
<extension-assigner>
<tag-type>provision-tag</tag-type>
```

```
</extension-assigner>
<fac>
<standard>true</standard>
<custom_list>
<custom_item>
<fac_string>callfwd all</fac_string>
<fac_list>**1</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>callfwd cancel</fac_string>
<fac_list>**2</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>pickup local</fac_string>
<fac_list>**3</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>pickup group</fac_string>
<fac_list>**4</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>pickup direct</fac_string>
<fac_list>**5</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>park</fac_string>
<fac_list>**6</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>dnd</fac_string>
<fac_list>**7</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>redial</fac_string>
<fac_list>**8</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>voicemail</fac_string>
<fac_list>**9</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>ephone-hunt join</fac_string>
<fac_list>*3</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>ephone-hunt cancel</fac_string>
<fac_list>#3</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>ephone-hunt hlog</fac_string>
<fac_list>*4</fac_list>
```

```
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>ephone-hunt hlog-phone</fac_string>
<fac_list>*5</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>trnsfvm</fac_string>
<fac_list>*6</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>dpark-retrieval</fac_string>
<fac_list>*0</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
<custom_item>
<fac_string>cancel call waiting</fac_string>
<fac_list>*1</fac_list>
<alias>0</alias>
<alias_map />
</custom_item>
</custom_list>
</fac>
<fxo>
<hook-flash>true</hook-flash>
</fxo>
<hunt-group>
<logout>HLog</logout>
<report>
<url_info>
<prefix>tftp://223.255.254.253/ngm/huntgp/2800/data</prefix>
<hg_suffix>
<low>-1</low>
<high>0</high>
</hg_suffix>
</url_info>
<delay>0</delay>
<duration>24</duration>
<internal>
<duration>5</duration>
<hg_suffix>
<low>1</low>
<high>5</high>
</hg_suffix>
</internal>
</report>
</hunt-group>
<internal-call>
<moh-group>-1</moh-group>
</internal-call>
<ip>
<qos>
<dscp_list>
<dscp_item>
<index>0</index>
<af11>media</af11>
</dscp_item>
<dscp_item>
<index>1</index>
<af12>signal</af12>
</dscp_item>
<dscp_item>
<index>2</index>
<af13>video</af13>
</dscp_item>
<dscp_item>
<index>3</index>
```

```
<af21>service</af21>
</dscp_item>
<dscp_item>
<index>4</index>
<af22>media</af22>
</dscp_item>
<dscp_item>
<index>5</index>
<af23>media</af23>
</dscp_item>
<dscp_item>
<index>6</index>
<af31>media</af31>
</dscp_item>
<dscp_item>
<index>7</index>
<af32>media</af32>
</dscp_item>
<dscp_item>
<index>8</index>
<af33>media</af33>
</dscp_item>
<dscp_item>
<index>9</index>
<af41>media</af41>
</dscp_item>
<dscp_item>
<index>10</index>
<af42>media</af42>
</dscp_item>
<dscp_item>
<index>11</index>
<af43>media</af43>
</dscp_item>
<dscp_item>
<index>12</index>
<cs1>media</cs1>
</dscp_item>
<dscp_item>
<index>13</index>
<cs2>media</cs2>
</dscp_item>
<dscp_item>
<index>14</index>
<cs3>media</cs3>
</dscp_item>
<dscp_item>
<index>15</index>
<cs4>media</cs4>
</dscp_item>
<dscp_item>
<index>16</index>
<cs5>media</cs5>
</dscp_item>
<dscp_item>
<index>17</index>
<cs6>media</cs6>
</dscp_item>
<dscp_item>
<index>18</index>
<cs7>media</cs7>
</dscp_item>
<dscp_item>
<index>19</index>
<default>media</default>
</dscp_item>
<dscp_item>
<index>20</index>
<ef>media</ef>
</dscp_item>
</dscp_list>
</qos>
<source-address>
```

```
<primary>10.4.188.90</primary>
<port>2000</port>
<secondary>1.4.188.90</secondary>
<rehome>0</rehome>
<strict-match>true</strict-match>
</source-address>
</ip>
<keepalive>
<timeout>30</timeout>
<aux_timeout>30</aux_timeout>
</keepalive>
<live-record>999</live-record>
<load_list>
<phone_7914>hehe</phone_7914>
<phone_7915-12>hehe</phone_7915-12>
<phone_7915-24>hehe</phone_7915-24>
<phone_7916-12>hehe</phone_7916-12>
<phone_7916-24>hehe</phone_7916-24>
<phone_12SP>hehe</phone_12SP>
<phone_7902>hehe</phone_7902>
<phone_7906>hehe</phone_7906>
<phone_7910>hehe</phone_7910>
<phone_7911>SCCP11.9-0-1FT6-4DEV</phone_7911>
<phone_7912>hehe</phone_7912>
<phone_7920>hehe</phone_7920>
<phone_7921>hehe</phone_7921>
<phone_7925>hehe</phone_7925>
<phone_7931>hehe</phone_7931>
<phone_7935>hehe</phone_7935>
<phone_7936>hehe</phone_7936>
<phone_7937>hehe</phone_7937>
<phone_7960-7940>P00308000501</phone_7960-7940>
<phone_7941>hehe</phone_7941>
<phone_7941GE>hehe</phone_7941GE>
<phone_7942>hehe</phone_7942>
<phone_7961>SCCP41.8-4-2-38S</phone_7961>
<phone_7962>hehe</phone_7962>
<phone_7965>hehe</phone_7965>
<phone_7970>hehe</phone_7970>
<phone_7971>hehe</phone_7971>
<phone_7975>hehe</phone_7975>
<phone_7985>hehe</phone_7985>
<phone_ata>hehe</phone_ata>
<phone_6921>hehe</phone_6921>
<phone_6941>hehe</phone_6941>
<phone_6961>hehe</phone_6961>
</load_list>
<load-cfg-file_list>
<load-cfg-file_item>
<cfg_file>flash:its/vrf1/XMLDefaultCIPC.cnf.xml</cfg_file>
<alias>cnf.xml</alias>
<sign>false</sign>
</load-cfg-file_item>
</load-cfg-file_list>
<log>
<table >
<max-size>150</max-size>
<retain-timer>15</retain-timer>
</table>
</log>
<login>
<timeout>60</timeout>
<clear>24:0</clear>
</login>
<max-conferences>
<count>8</count>
<gain>-6</gain>
</max-conferences>
<max-dn>
<count>180</count>
<global_preference>0</global_preference>
<no-reg>secondary</no-reg>
</max-dn>
```

```
<max-ephones>48</max-ephones>
<max-redirect>10</max-redirect>
<modem>
<passthrough>
<payload-type>100</payload-type>
</passthrough>
<relay_sse>
<payload-type>118</payload-type>
</relay_sse>
<relay_sprt>
<payload-type>120</payload-type>
</relay_sprt>
</modem>
<moh_file>flash:music-on-hold.au</moh_file>
<moh-file-buffer>10000</moh-file-buffer>
<multicast>
<moh_ipaddr>239.10.10.10</moh_ipaddr>
<port>2000</port>
<route_list>
<route_item>
<index>1</index>
<route>10.10.10.10</route>
</route_item>
</route_list>
</multicast>
<mwi-server>
<prefix />
<reg-e164>true</reg-e164>
<relay>true</relay>
</mwi-server>
<network-locale_list>
<network-locale_item>
<index>0</index>
<locale>US</locale>
</network-locale_item>
<network-locale_item>
<index>1</index>
<locale>US</locale>
</network-locale_item>
<network-locale_item>
<index>2</index>
<locale>US</locale>
</network-locale_item>
<network-locale_item>
<index>3</index>
<locale>US</locale>
</network-locale_item>
<network-locale_item>
<index>4</index>
<locale>US</locale>
</network-locale_item>
</network-locale_list>
<night-service>
<option>everyday</option>
<code>*234</code>
<date_list>
<date_item>
<index>1</index>
<month>Jan</month>
<day_of_month>1</day_of_month>
<start_time>12:00</start_time>
<stop_time>14:00</stop_time>
</date_item>
</date_list>
<day_list>
<day_item>
<index>1</index>
<day_of_week>Sun</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
<day_item>
<index>2</index>
```

```
<day_of_week>Mon</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
<day_item>
<index>3</index>
<day_of_week>Tue</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
<day_item>
<index>4</index>
<day_of_week>Wed</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
<day_item>
<index>5</index>
<day_of_week>Thu</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
<day_item>
<index>6</index>
<day_of_week>Fri</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
<day_item>
<index>7</index>
<day_of_week>Sat</day_of_week>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</day_item>
</day_list>
<everyday>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</everyday>
<weekday>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</weekday>
<weekend>
<start_time>12:00</start_time>
<stop_time>16:00</stop_time>
</weekend>
</night-service>
<pin>1234</pin>
<pin_override>true</pin_override>
<privacy>true</privacy>
<privacy-on-hold>false</privacy-on-hold>
<protocol>
<mode>dual-stack</mode>
<preference>ipv4</preference>
</protocol>
<sdspfarm>
<conference_options>
<mute-on>124</mute-on>
<mute-off>234</mute-off>
<hardware>false</hardware>
</conference_options>
<units>4</units>
<tag_list>
<tag_item>
<tag>1</tag>
<device>mtp-conf</device>
</tag_item>
</tag_list>
<transcode>
<sessions>4</sessions>
</transcode>
<unregister>
```

```
<force>1</force>
</unregister>
</sdspfarm>
<secondary-dialtone>4567</secondary-dialtone>
<secure-signaling>
<trustpoint />
</secure-signaling>
<server-security-mode />
<service>
<local-directory>true</local-directory>
<local-directory_authenticate>false</local-directory_authenticate>
<dss>false</dss>
<dnis>
<overlay>false</overlay>
<dir-lookup>false</dir-lookup>
</dnis>
<directed-pickup>true</directed-pickup>
<directed-pickup_gpickup>false</directed-pickup_gpickup>
<phone_list>
<phone_item>
<index>1</index>
<phone_params>displayOnTime</phone_params>
<phone_text>time.xml</phone_text>
</phone_item>
</phone_list>
</service>
<ssh>
<userid>ngm</userid>
<password>ngm</password>
</ssh>
<standby>
<user>ngm</user>
<password>ngm</password>
</standby>
<system_message>LITTLE TWIN STARS (2800)</system_message>
<tftp-server-credentials>
<trustpoint />
</tftp-server-credentials>
<time-format>12</time-format>
<time-webedit>false</time-webedit>
<time-zone>0</time-zone>
<timeouts>
<busy_timeout>10</busy_timeout>
<interdigit_timeout>10</interdigit_timeout>
<ringing_timeout>180</ringing_timeout>
<transfer-recall_timeout>0</transfer-recall_timeout>
<night-service-bell_timeout>12</night-service-bell_timeout>
</timeouts>
<transfer-digit-collect>new-call</transfer-digit-collect>
<transfer-pattern_list>
<transfer-pattern_item>
<index>1</index>
<pattern>....</pattern>
<blind>false</blind>
</transfer-pattern_item>
<transfer-pattern_item>
<index>2</index>
<pattern>.T</pattern>
<blind>false</blind>
</transfer-pattern_item>
</transfer-pattern_list>
<transfer-system>
<type>full-consult</type>
<dss>false</dss>
</transfer-system>
<trunk_optimization_pre_connect>false</trunk_optimization_pre_connect>
<url_list>
<information>
<url>http://1.4.188.101/localdir</url>
</information>
<directories>
<url>http://1.4.188.101/localdir</url>
</directories>
```

```
<messages>
<url>http://1.4.188.101/localdir</url>
</messages>
<services>
<url>http://1.4.188.101/localdir</url>
<name />
</services>
<proxy_server>
<url>http://1.4.188.101/localdir</url>
</proxy_server>
<idle>
<url>http://1.4.188.101/localdir</url>
<idle_timeout>90</idle_timeout>
</idle>
<authentication>
<url>http://1.4.188.101/localdir</url>
<user />
<password />
</authentication>
</url_list>
<user-locale_list>
<user-locale_item>
<index>0</index>
<locale>US</locale>
<package>en</package>
<load >
</user-locale_item>
<user-locale_item>
<index>1</index>
<locale>US</locale>
<package>en</package>
<load />
</user-locale_item>
<user-locale_item>
<index>2</index>
<locale>US</locale>
<package>en</package>
<load />
</user-locale_item>
<user-locale_item>
<index>3</index>
<locale>US</locale>
<package>en</package>
<load />
</user-locale_item>
<user-locale_item>
<index>4</index>
<locale>US</locale>
<package>en</package>
<load />
</user-locale_item>
</user-locale_list>
<video>
<maximum>
<bit-rate>10000000</bit-rate>
</maximum>
</video>
<voicemail>6050</voicemail>
<web>
<system_admin>
<name>Admin</name>
<secret>-1</secret>
<password />
</system_admin>
<customer_admin>
<name>ngm</name>
<secret>5</secret>
<password>$1$.nfD$zn3h3bp/4grULFS87ZHHV/</password>
</customer_admin>
<customize>
<load />
</customize>
</web>
```

```
<xml>
<user>cisco</user>
<password>cisco</password>
<level>0</level>
</xml>
</ISGlobal>
</response>
```

ISgetDevice

Use ISgetDevice to retrieve configuration and status information for IP phones.

Use any combination of the following parameters in the request message to specific one or more SCCP phones:

- ISDevID with the ephone tag number of SCCP phone to be queried.
- ISDevName with the MAC address of SCCP phone to be queried.
- ISKeyword with one of the following options:
  - all—All configured SCCP phones
  - allTag—Ephone tag numbers for all SCCP phones configured
  - available—Next available ephone tag number to be configured

Request:

```
<request xsi:type="ISgetDevice">
<ISgetDevice>
<ISDevID>1</ISDevID>
<ISDevName>SEP0012DA8AC43D</ISDevName>
<ISDevName>allKeyphone</ISDevName>
</ISgetDevice>
</request>
```

Response

```
<response>
<ISDevices>
<ISDevice>
<ISDevID>1</ISDevID>
<ISDevName>SEP0016C7C7AF9D</ISDevName>
<ISDevType>Others</ISDevType>
<ISconfigDevType>7911</ISconfigDevType>
<ISDevUsername>test</ISDevUsername>
<ISDevLineButtons>
<ISDevLineButton>
<ISDevLineButtonID>1</ISDevLineButtonID>
<ISDevLineButtonMode>MONITOR_RING</ISDevLineButtonMode>
</ISDevLineButton>
</ISDevLineButtons>
<after-hours_exempt>false</after-hours_exempt>
<after-hours_login>
<http>false</http>
</after-hours_login>
<block-blind-xf-fallback>false</block-blind-xf-fallback>
<capf-ip-in-cnf>false</capf-ip-in-cnf>
<codec>
<codec_name>g711ulaw</codec_name>
<dspfarm-assist>false</dspfarm-assist>
</codec>
<adhoc_conference>
<add-mode>
```

```
<creator>true</creator>
</add-mode>
<admin>true</admin>
<drop-mode>
<creator>false</creator>
<local>false</local>
</drop-mode>
</adhoc_conference>
<fastdial_list>
<fastdial_item>
<fastdial>1</fastdial>
<fastdial_number>1234</fastdial_number>
<fastdial_name>home LINE</fastdial_name>
</fastdial_item>
</fastdial_list>
<feature-button_list>
<feature-button_item>
<feature-button>1</feature-button>
<feature_type>Dnd</feature_type>
</feature-button_item>
<feature-button_item>
<feature-button>2</feature-button>
<feature_type>Flash</feature_type>
</feature-button_item>
</feature-button_list>
<keep-conference>
<hangup>true</hangup>
<drop-last>false</drop-last>
<endcall>true</endcall>
<local-only>true</local-only>
</keep-conference>
<keypad-normalize>false</keypad-normalize>
<keyphone>false</keyphone>
<mtp>true</mtp>
<multicast-moh>true</multicast-moh>
<night-service_bell>true</night-service_bell>
<privacy />
<privacy-button>false</privacy-button>
<transfer-park>
<blocked>false</blocked>
</transfer-park>
<transfer-pattern>
<blocked>false</blocked>
</transfer-pattern>
<busy-trigger-per-button>0</busy-trigger-per-button>
<emergency-resp_location>0</emergency-resp_location>
<max-calls-per-button>0</max-calls-per-button>
<nte-end-digit-delay>0</nte-end-digit-delay>
<keepalive>
<timeout>30</timeout>
<aux_timeout>30</aux_timeout>
</keepalive>
<lpcor>
<type>none</type>
</lpcor>
<exclude-services>
<em_service>true</em_service>
<directory_service>false</directory_service>
<myphoneapp_service>false</myphoneapp_service>
</exclude-services>
<park>
<reservation-group>park</reservation-group>
</park>
<paging-dn>
<dn>0</dn>
<mode>multicast</mode>
</paging-dn>
<speed-dial_list>
<speed-dial_item>
<index>1</index>
<phone_number>1234</phone_number>
<label>home</label>
</speed-dial_item>
```

```
</speed-dial_list>
<ssh>
<userid>ngm</userid>
<password>ngm</password>
</ssh>
<phone_type>
<name>7911</name>
<addon_list>
<addon_item>
<addon>1</addon>
<addon_type>7914</addon_type>
</addon_item>
</addon_list>
</phone_type>
<auto-line>
<mode>normal</mode>
<auto_select_line>0</auto_select_line>
</auto-line>
<blf-speed-dial_list>
<blf-speed-dial_item>
<index>1</index>
<phone_number>1234</phone_number>
<label>blfsd</label>
</blf-speed-dial_item>
<device>true</device>
</blf-speed-dial_list>
<bulk-speed-dial_list>
<bulk-speed-dial_item>
<list>1</list>
<url />
</bulk-speed-dial_item>
</bulk-speed-dial_list>
<capf-auth-str>7777</capf-auth-str>
<description>ephoneOne</description>
<device-security-mode>none</device-security-mode>
<dnd>
<feature-ring>true</feature-ring>
</dnd>
<ephone-template>1</ephone-template>
<headset>
<auto-answer>
<line_list>
<line>1</line>
</line_list>
</auto-answer>
</headset>
<logout-profile>0</logout-profile>
<display_all_missed_calls>true</display_all_missed_calls>
<mwi-line>1</mwi-line>
<offhook-guard-timer>0</offhook-guard-timer>
<phone-ui>
<snr>true</snr>
<speeddial-fastdial>true</speeddial-fastdial>
</phone-ui>
<pin>1234</pin>
<presence>
<call-list>true</call-list>
</presence>
<provision-tag>1</provision-tag>
<username>test</username>
<password>test</password>
<video_enable>true</video_enable>
<vm-device-id>SEP0016C7C7AF9D</vm-device-id>
<ISDevAddr>
<Xipv4Address>0.0.0.0</Xipv4Address>
</ISDevAddr>
<ISPhoneLineList>
<ExtMapStatus>
<LineId>1</LineId>
<ExtId>176</ExtId>
<ExtNumber>6176</ExtNumber>
<ExtStatus>false</ExtStatus>
<LineState>idle</LineState>
```

```
</ExtMapStatus>
</ISPhoneLineList>
<ISKeyPhone>false</ISKeyPhone>
<SNRui>true</SNRui>
<ISLogoutProfileID>0</ISLogoutProfileID>
<ISUserProfileID>0</ISUserProfileID>
<ISTapiClientAddr>
<Xipv4Address />
</ISTapiClientAddr>
<ISDevStatus>unregistered</ISDevStatus>
<ISDevLastStatus>deceased</ISDevLastStatus>
<ISDevChangeTime>4040</ISDevChangeTime>
<ISDevKeepAlives>0</ISDevKeepAlives>
<ISDevTapiCStatus />
<ISTapiCLastStatus />
<ISTapiCChangeTime />
<ISTapiCKeepAlive />
<ISDevDND>no</ISDevDND>
</ISDevice>
</ISDevices>
</response>
```

ISgetDeviceTemplate

Use ISgetDeviceTemplate to retrieve configuration and status information for IP phone templates.

Use any combination of the following parameters in the request message to specify one or more phone templates:

- ISDevTemplateID with phone template tag number to be queried.
- ISKeyword with one of the following options:
  - all—All configured phone templates
  - allTag—Phone template tag numbers for all configured phone templates
  - available—Next available phone template tag number to be configured

Request

```
<request>
<ISgetDeviceTemplate>
<ISgetDevTemplateID>1</ISgetDevTemplateID>
<ISgetDeviceTemplate>
</request>
```

Response

```
<response>
<ISDeviceTemplates>
<ISDeviceTemplate>
<ISDevTemplateID>1<ISDevTemplateID>
<after-hours>
<block_list>
<block_item>
<pattern_id>1<pattern_id>
<blocking_pattern>1234<blocking_pattern>
<blocking_option>7-24<blocking_option>
<block_item>
<block_list>
<date_list>
<date_item>
<month>Jan<month>
```

```
<day_of_month>1<day_of_month>
<start_time>12:00<start_time>
<stop_time>14:00<stop_time>
<date_item>
<date_list>
<day_list>
<day_item>
<day_of_week>Mon<day_of_week>
<start_time>12:00<start_time>
<stop_time>14:00<stop_time>
<day_item>
<day_list>
<exempt>true<exempt>
<after-hours_login>
<http>true<http>
<after-hours_login>
<override-code>1234<override-code>
<after-hours>
<block-blind-xf-fallback>false<block-blind-xf-fallback>
<button-layout_phone_7931>0<button-layout_phone_7931>
<button-layout_list>
<button-layout_item>
<button-layout>1,9<button-layout>
<button-type>line<button-type>
<button-layout_item>
<button-layout_item>
<button-layout>4-5,7<button-layout>
<button-type>speed-dial<button-type>
<button-layout_item>
<button-layout_item>
<button-layout>2-3<button-layout>
<button-type>feature<button-type>
<button-layout_item>
<button-layout_item>
<button-layout>11<button-layout>
<button-type>url<button-type>
<button-layout_item>
<button-layout_list>
<capf-ip-in-cnf>false<capf-ip-in-cnf>
<codec>
<codec_name>g711ulaw<codec_name>
<dspfarm-assist>false<dspfarm-assist>
<codec>
<adhoc_conference>
<add-mode>
<creator>false<creator>
<add-mode>
<admin>false<admin>
<drop-mode>
<creator>false<creator>
<local>false<local>
<drop-mode>
<adhoc_conference>
<fastdial_list>
<fastdial_item>
<fastdial>1<fastdial>
<fastdial_number>1234<fastdial_number>
<fastdial_name>office<fastdial_name>
<fastdial_item>
<fastdial_list>
<feature-button_list>
<feature-button_item>
<feature-button>1<feature-button>
<feature_type>HLog<feature_type>
<feature-button_item>
<feature-button_item>
<feature-button>2<feature-button>
<feature_type>Park<feature_type>
<feature-button_item>
<feature-button_item>
<feature-button>3<feature-button>
<feature_type>Privacy<feature_type>
<feature-button_item>
```

```
<feature-button_list>
<url-button_list>
<url-button_item>
<url-button>1<url-button>
<url-button_type>em<url-button_type>
<url-button_item>
<url-button_item>
<url-button>3<url-button>
<url-button_type>myphoneapp<url-button_type>
<url-button_item>
<url-button_item>
<url-button>6<url-button>
<url-button_type>service<url-button_type>
<url-button_url>hello<url-button_url>
<url-button_name>helloworld<url-button_name>
<url-button_item>
<url-button_list>
<features_blocked>Pickup Park GPickup<features_blocked>
<keep-conference>
<hangup>false<hangup>
<drop-last>false<drop-last>
<endcall>false<endcall>
<local-only>false<local-only>
<keep-conference>
<keypad-normalize>false<keypad-normalize>
<keyphone>false<keyphone>
<mlpp>
<indication>true<indication>
<preemption>true<preemption>
<max_priority>-1<max_priority>
<mlpp>
<mtp>false<mtp>
<multicast-moh>true<multicast-moh>
<night-service_bell>false<night-service_bell>
<privacy >
<privacy-button>false<privacy-button>
<phone_service>
<param_list>
<param_item>
<param>displayOnTime<param>
<text>170<text>
<param_item>
<param_list>
<phone_service>
<softkeys>
<alerting_keys >
<connected_keys >
<hold_keys >
<idle_keys >
<remote-in-use_keys>CBarge Newcall<remote-in-use_keys>
<ringing_keys >
<seized_keys >
<softkeys>
<transfer-park>
<blocked>false<blocked>
<transfer-park>
<transfer-pattern>
<blocked>false<blocked>
<transfer-pattern>
<busy-trigger-per-button>0<busy-trigger-per-button>
<emergency-resp_location>0<emergency-resp_location>
<max-calls-per-button>0<max-calls-per-button>
<network_locale>0<network_locale>
<nte-end-digit-delay>0<nte-end-digit-delay>
<transfer_max-length>0<transfer_max-length>
<user_locale>0<user_locale>
<keepalive>
<timeout>30<timeout>
<aux_timeout>30<aux_timeout>
<keepalive>
<lpcor>
<type>none<type>
<lpcor>
```

```
<exclude-services>
<em_service>false<em_service>
<directory_service>true<directory_service>
<myphoneapp_service>true<myphoneapp_service>
<exclude-services>
<park>
<reservation-group>1234<reservation-group>
<park>
<paging-dn>
<dn>0<dn>
<mode>multicast<mode>
<paging-dn>
<speed-dial_list>
<speed-dial_item>
<index>1<index>
<phone_number>1234<phone_number>
<label>play<label>
<speed-dial_item>
<speed-dial_list>
<ssh>
<userid>test<userid>
<password>test<password>
<ssh>
<phone_type>
<name>7960<name>
<addon_list>
<addon_item>
<addon>1<addon>
<addon_type>7914<addon_type>
<addon_item>
<addon_list>
<phone_type>
<url_services_list>
<url_services_item>
<services_id>1<services_id>
<url>http<url>
<name>HTTP<name>
<url_services_item>
<url_services_list>
<ISDeviceTemplate>
<ISDeviceTemplates>
<response>
```

ISgetExtension

Use ISgetExtension to retrieve configuration and status information for extension numbers.

Use any combination of the following parameters in the request message to specify one or more extensions:

- ISExtID with the extension ID number to be queried.
- ISExtNumber with the extension number to be queried.
- ISKeyword with one of the following options:
  - all—Displays details of all extension numbers configured
  - allTag—Displays a list of all extension ID numbers configured
  - available—Next available extension ID number to be configured

Request

```
<request>
<ISExtension>
<ISVExtID>1</ISExtID>
```

```
<ISExtNumber>1</ISExtNumber>
</ISExtension>
</request>
```

Response

```
<response>
<ISExtensions>
<ISExtension>
<ISExtID>1</ISExtID>
<ISExtNumber>6001</ISExtNumber>
<ISExtSecNumber>6111</ISExtSecNumber>
<ISExtType>normal</ISExtType>
<ISExtStatus>up</ISExtStatus>
<ISExtChangeTime>3122733</ISExtChangeTime>
<ISExtUsage>0</ISExtUsage>
<ISExtHomeAddress>0.0.0.0</ISExtHomeAddress>
<ISExtMultiLines>0</ISExtMultiLines>
<ISExtPortName>EFXS 50/0/1</ISExtPortName>
<ISExtLineMode>DUAL_LINE</ISExtLineMode>
<ISExtCallStatus>IDLE</ISExtCallStatus>
<Mobility>false</Mobility>
<SNRnumber>1111</SNRnumber>
<SNRdelay>10</SNRdelay>
<SNRtimeout>5</SNRtimeout>
<SNRnoanNumber />
<ISAllowWatch>true</ISAllowWatch>
<ISSessionServerIDs>
<ISSessionServerID>1</ISSessionServerID>
</ISSessionServerIDs>
<firstName />
<lastName>ephoneDnOne</lastName>
<callForwardAll>1234</callForwardAll>
<ISDevList>
<ISDeviceID>8</ISDeviceID>
</ISDevList>
<allow>
<watch>true</watch>
</allow>
<call-forward>
<all>
<number>1234</number>
</all>
<busy>
<number>9000</number>
<option>secondary</option>
<dialplan-pattern>false</dialplan-pattern>
</busy>
<max-length>
<number />
</max-length>
<night-service-activated>
<number>2323</number>
</night-service-activated>
<noan>
<number>1234</number>
<timeout>80</timeout>
<dialplan-pattern>true</dialplan-pattern>
<option />
</noan>
</call-forward>
<call-waiting>
<cw_beep>
<accept>true</accept>
<generate>true</generate>
</cw_beep>
<cw_ring>true</cw_ring>
</call-waiting>
<corlist>
<incoming />
<outgoing />
```

```
</corlist>
<cti>
<notify>true</notify>
<watch>true</watch>
</cti>
<description>ephoneDnOne</description>
<hold-alert>
<timeout>15</timeout>
<mode>idle</mode>
<ring-silent-dn>true</ring-silent-dn>
</hold-alert>
<huntstop>
<channel>8</channel>
</huntstop>
<moh-group>0</moh-group>
<mwi>
<type>qsig</type>
<mode />
</mwi>
<mwi-type>both</mwi-type>
<pickup-group />
<transfer-recall_timeout>0</transfer-recall_timeout>
<translate>
<called>1</called>
<calling>2</calling>
</translate>
<translation-profile>
<incoming>in</incoming>
<outgoing>out</outgoing>
</translation-profile>
<application>
<name>calling</name>
<out-bound>calling</out-bound>
</application>
<port-caller-id>
<block>false</block>
<local>false</local>
<transfer_passthrough>false</transfer_passthrough>
</port-caller-id>
<conference_dn>
<mode />
<unlocked>false</unlocked>
</conference_dn>
<ephone-dn-template>0</ephone-dn-template>
<ephone-hunt_login>true</ephone-hunt_login>
<feed>
<ip_addr>0.0.0.0</ip_addr>
<port>0</port>
<route>0.0.0.0</route>
<out-call />
</feed>
<fwd-local-calls>true</fwd-local-calls>
<intercom>
<dn-plar />
<barge-in>false</barge-in>
<label />
<no-mute>true</no-mute>
<ptt>false</ptt>
<no-auto-answer>true</no-auto-answer>
</intercom>
<label />
<loopback-dn>
<dn>0</dn>
<auto-con>false</auto-con>
<loopback-codec />
<forward>0</forward>
<prefix />
<retry>0</retry>
<strip>0</strip>
<suffix />
</loopback-dn>
<mailbox-selection>
<last-redirect-num>false</last-redirect-num>
```

```
</mailbox-selection>
<moh>
<ip_addr>0.0.0.0</ip_addr>
<port>0</port>
<route>0.0.0.0</route>
<out-call />
</moh>
<name>ephoneDnOne</name>
<night-service_bell>false</night-service_bell>
<telephony_number>
<primary>6001</primary>
<secondary>6111</secondary>
<no-reg>true</no-reg>
<no-reg_option />
</telephony_number>
<paging>
<group />
<ip_addr>0.0.0.0</ip_addr>
<port>0</port>
</paging>
<park-slot>
<directed>false</directed>
<reserved-for />
<reservation-group />
<timeout>0</timeout>
<limit>0</limit>
<notify />
<only>false</only>
<transfer_destination />
<recall>true</recall>
<alternate />
<retry>0</retry>
<retry_limit>0</retry_limit>
</park-slot>
<pickup-call>
<any-group>false</any-group>
</pickup-call>
<dn_preference>
<order>0</order>
<secondary>9</secondary>
</dn_preference>
<queueing-dn>
<mode />
<timeout>180</timeout>
<transfer_number />
</queueing-dn>
<ring>
<type>external</type>
<line>primary</line>
</ring>
<session-server>
<server>1</server>
</session-server>
<snr_info>
<value>1111</value>
<delay>10</delay>
<timeout>5</timeout>
<cfwd-noan />
</snr_info>
<transfer-mode />
<trunk>
<number />
<timeout>3</timeout>
<transfer-timeout>0</transfer-timeout>
<monitor-port />
</trunk>
<whisper-intercom>
<speed-dial />
<label />
</whisper-intercom>
</ISExtension>
</ISExtensions>
</response>
```

ISgetExtensionTemplate

Use the ISgetExtensionTemplates to retrieve configuration and status information for extension templates.

Use any combination of the following parameters in the request message to specify one or more extensions:

- ISExtTemplateID with the extension template ID number to be queried.
- ISKeyword with one of the following options:
  - all—Displays details of all configured extension templates
  - allTag—Displays a list of all configured extension template ID numbers
  - available—Next available extension template ID number to be configured

Request

```
<request>
<ISExtensionTemplates>
<ISExtensionTemplateID>1</ISExtensionTemplateID>
</ISgetExtensionTemplate>
</request>
```

Response

```
<response>
<ISExtensionTemplates>
<ISExtensionTemplate>
<ISExtTemplateID>1</ISExtTemplateID>
<allow>
<watch>false</watch>
</allow>
<call-forward>
<all>
<number>1234</number>
</all>
<busy>
<number>3456</number>
<option>primary</option>
<dialplan-pattern>false</dialplan-pattern>
</busy>
<max-length>
<number>4</number>
</max-length>
<night-service-activated>
<number>7777</number>
</night-service-activated>
<noan>
<number>9999</number>
<timeout>80</timeout>
<dialplan-pattern>false</dialplan-pattern>
<option>secondary<option>
</noan>
</call-forward>
<call-waiting>
<cw_beep>
<accept>true</accept>
<generate>true</generate>
</cw_beep>
<cw_ring>true</cw_ring>
</call-waiting>
<caller-id_blocked>true</caller-id_blocked>
<corlist>
```

```
<incoming />
<outgoing />
</corlist>
<cti>
<notify>false</notify>
<watch>false</watch>
</cti>
<description>ephoneDnTemplate</description>
</hold-alert>
<timeout>15</timeout>
<mode>idle</mode>
<ring-silent-dn>true</ring-silent-dn>
</hold-alert>
<huntstop>
<channel>8</channel>
</huntstop>
<moh-group>0</moh-group>
<mwi>
<type>sip</type>
<mode>on-off</mode>
</mwi>
<mwi-type>both</mwi-type>
<pickup-group>1</pickup-group>
<transfer-recall_timeout>400</transfer-recall_timeout>
<translate>
<called>1</called>
<calling>0</calling>
</translate>
<translation-profile>
<incoming>1</incoming>
<outgoing>1</outgoing>
</translation-profile>
</ISExtensionTemplate>
</ISExtensionTemplates>
</response>
```


ISgetUser

Use ISgetUser to retrieve information for a particular user in Cisco Unified CME. The request must include the ISuserID parameter with a user name that is configured in Cisco Unified CME. If the request contains a valid ISuserID, the response includes the user-name tag number (ISuserTag) and type for this user.

The value for ISuserType corresponds to how a username is configured in Cisco Unified CME, as follows:

- 0—INVALID_CME_USER
- 1—EPHONE_USER
- 2—LOGOUT_PROFILE_USER
- 3—USER_PROFILE_USER

If the request contains an invalid ISuserID, the value for ISuserTag and ISuserType will both be “0.”

Request

```
<request>
<ISgetUser>
<ISuserID>a</ISuserID>
</ISgetUser>
</request>
```

Response

```
<response>
<ISuser>
<ISuserID>a</ISuserID>
<ISuserType>3</ISuserType>
<ISuserTag>1</ISuserTag>
</ISuser>
</response>
```

ISgetUserProfile

Use the ISgetUserProfile to retrieve the status and configuration information for a specific user profile.

Use any combination of the following:

- ISUserProfileID with the user profile ID of a specific user.
- ISuserID with user ID of a specific user.
- ISKeyword with one of the following options:
  - all—Displays details of all configured user profiles.
  - allTag—Displays a list of all configured user profile IDs.
  - available—Next available user profile.

Request

```
<request>
<ISgetUserProfile>
<ISUserProfileID>1</ISUserProfileID>
</ISgetUserProfile>
</request>
```

Response

```
<response>
<ISUserProfiles>
<ISUserProfile>
<ISUserProfileID>1</ISUserProfileID>
<ISuserID>a</ISuserID>
<ISpassword>a</ISpassword>
<ISuserPin>12</ISuserPin>
<ISPrivacyButton>no</ISPrivacyButton>
<ISuserMaxIdleTime>0</ISuserMaxIdleTime>
<SpeedDials>
<SpeedDial>
<SpeedDialIndex>1</SpeedDialIndex>
<SpeedDialNumber>901</SpeedDialNumber>
<SpeedDialLabel />
<SpeedDialBLF>no</SpeedDialBLF>
</SpeedDial>
<SpeedDial>
<SpeedDialIndex>2</SpeedDialIndex>
<SpeedDialNumber>902</SpeedDialNumber>
<SpeedDialLabel />
<SpeedDialBLF>no</SpeedDialBLF>
</SpeedDial>
<SpeedDial>
<SpeedDialIndex>3</SpeedDialIndex>
<SpeedDialNumber>2002</SpeedDialNumber>
```

```
<SpeedDialLabel>2002Label</SpeedDialLabel>
<SpeedDialBLF>no</SpeedDialBLF>
</SpeedDial>
<SpeedDial>
<SpeedDialIndex>5</SpeedDialIndex>
<SpeedDialNumber>2004</SpeedDialNumber>
<SpeedDialLabel>2004</SpeedDialLabel>
<SpeedDialBLF>yes</SpeedDialBLF>
</SpeedDial>
</SpeedDials>
<UserNumbers>
<UserNumber>
<ISExtNumber>2003</ISExtNumber>
<ISExtMode>NORMAL</ISExtMode>
<ISExtOverlayGroup>0</ISExtOverlayGroup>
<ISExtCombo>no</ISExtCombo>
</UserNumber>
<UserNumber>
<ISExtNumber>201</ISExtNumber>
<ISExtMode>NORMAL</ISExtMode>
<ISExtOverlayGroup>0</ISExtOverlayGroup>
<ISExtCombo>no</ISExtCombo>
</UserNumber>
<UserNumber>
<ISExtNumber>202</ISExtNumber>
<ISExtMode>NORMAL</ISExtMode>
<ISExtOverlayGroup>0</ISExtOverlayGroup>
<ISExtCombo>no</ISExtCombo>
</UserNumber>
</UserNumbers>
<ISuserCurrentPhone>
<CurrentPhoneType>Unknown</CurrentPhoneType>
<CurrentPhoneID>0</CurrentPhoneID>
</ISuserCurrentPhone>
</ISUserProfile>
</ISUserProfiles>
</response>
```

ISgetUtilityDirectory

Use the ISgetUtilityDirectory to retrieve status and configuration information for directory information.

Request

```
<request>
<ISgetUtilityDirectory>
</ISgetUtilityDirectory>
</request>
```

Response

```
<response>
<ISUtilityDirectory>
<ISDirectoryEntry>
<ISDirectoryTag>1</ISDirectoryTag>
<ISDirectoryNumber>12345</ISDirectoryNumber>
<firstName>first</firstName>
<lastName>last</lastName>
</ISDirectoryEntry>
<ISDirectoryEntry>
<ISDirectoryTag>2</ISDirectoryTag>
<ISDirectoryNumber>67890</ISDirectoryNumber>
<firstName>first2</firstName>
<lastName>last 2</lastName>
</ISDirectoryEntry>
</ISUtilityDirectory>
</response>
```

ISgetVoiceRegGlobal

Use the ISgetVoiceRegGlobal to retrieve status and configuration information of global parameters for SIP,

Request

```
<request>
<ISgetVoiceRegGlobal>
</ISgetVoiceRegGlobal>
</request>
```

Response

```
<response>
<ISSipGlobal>
<ISAddress>10.10.10.1</ISAddress>
<ISMode>cme</ISMode>
<ISVersion>7.1</ISVersion>
<ISAuthModes>
<ISAuthMode>ood_refer</ISAuthMode>
<ISAuthMode>presence</ISAuthMode>
</ISAuthModes>
<ISPortNumber>5060</ISPortNumber>
<ISMaxPool>10</ISMaxPool>
<ISMaxDN>100</ISMaxDN>
<ISMaxRedirect>5</ISMaxRedirect>
</ISSipGlobal>
</response>
```

ISgetSipDevice

For SIP phones, use any combination of the following parameters in the request message to specify one or more SIP phones:

- ISPoolID with the voice register pool tag number of SIP phone to be queried.
- ISPoolName with the voice register pool name of the SIP phone to be queried.
- ISKeyword with one of the following options:
  - all—All configured SIP phones
  - allTag—Voice register pool tag numbers for all configured SIP phones
  - available—Next available phone tag number to be configured

Request

```
<request>
<ISgetSipDevice>
<ISPoolID>1</ISPoolID>
</ISgetSipDevice>
</request>
```

Response

```
<response>
<ISSipDevices>
```

```
<ISSipDevice>
<ISPoolID>1</ISPoolID>
<ISDevMac>0013.1978.3CA5</ISDevMac>
<ISSessionServerID>0</ISSessionServerID>
<ISDevAddr>
<Xipv4Address>0</Xipv4Address>
</ISDevAddr>
<ISSipPhoneLineList>
<ExtMapStatus>
<LineId>1</LineId>
<ExtId>1</ExtId>
<ExtNumber>901</ExtNumber>
<LineState>idle</LineState>
</ExtMapStatus>
<ExtMapStatus>
<LineId>2</LineId>
<ExtId>2</ExtId>
<ExtNumber>902</ExtNumber>
<LineState>idle</LineState>
</ExtMapStatus>
</ISSipPhoneLineList>
<ISPoolMaxRegistration>42</ISPoolMaxRegistration>
<ISPoolDtmfRelay>rtp-nte</ISPoolDtmfRelay>
<ISDevCodec>g729r8</ISDevCodec>
</ISSipDevice>
</ISSipDevices>
</response>
```

ISgetSipExtension

Use ISgetSipExtension to retrieve configuration and status information for extension numbers.

Use any combination of the following parameters in the request message to specify one or more extensions:

- ISVoiceRegDNID with the extension ID number to be queried.
- ISVoiceRegNumber with the extension number to be queried.
- ISKeyword with one of the following options:
    - all—Displays details of all configured extension numbers
    - allTag—Displays a list of all configured extension ID numbers
    - available—Next available extension ID number to be configured

Request

```
<request>
<ISgetSipExtension>
<ISVoiceRegDNID>1</ISVoiceRegDNID>
</ISgetSipExtension>
</request>
```

Response

```
<response>
<ISSipExtensions>
<ISSipExtension>
<ISVoiceRegDNID>1</ISVoiceRegDNID>
<ISExtNumber>901</ISExtNumber>
<ISSessionServerIDs>
<ISSessionServerID>1</ISSessionServerID>
<ISSessionServerID>2</ISSessionServerID>
```

```
</ISSessionServerIDs>
<ISAllowWatch>true</ISAllowWatch>
<firstName>Henry</firstName>
<lastName>Mann</lastName>
<ISSipDevList>
<ISPoolID>1</ISPoolID>
<ISPoolID>2</ISPoolID>
</ISSipDevList>
</ISSipExtension>
</ISSipExtensions>
</response>
```

ISgetSessionServer

Use ISgetSessionServer to retrieve configuration information for session servers in Cisco Unified CME.

Use any combination of the following parameters in the request message to specify one or more session servers:

- ISSessionServerID with the session server tag number.
- ISSessionserverName with session server name.
- ISKeyword with one of the following keywords:
    - all—All configured session servers
    - allTag—Session server tag numbers for all configured session servers
    - available—Next available session server tag number to be configured

Request

```
<request>
<ISgetSessionServer>
<ISSessionServerID>1</ISSessionServerID>
</ISgetSessionServer>
</request>
```

Response

```
<response>
<ISSessionServers>
<ISSessionServer>
<ISSessionServerID>1</ISSessionServerID>
<ISSessionRegisterID>SS1</ISSessionRegisterID>
<ISSessionKeepAlives>60</ISSessionKeepAlives>
</ISSessionServer>
</ISSessionServers>
</response>
```

ISgetVoiceHuntGroup

Use the ISgetVoiceHuntGroupID to retrieve status and configuration information for voice hunt groups.

Use any combination of the following parameters in the request message to specify one or more voice hunt groups:

- ISVoiceHuntGroupID with the voice hunt group ID number.

- ISKeyword with one of the following keywords:
    - all—All configured voice hunt groups
    - allTag—Voice hunt group ID numbers for all configured voice hunt groups
    - available—Next available voice hunt group ID number to be configured

Request

```
<request>
<ISgetVoiceHuntGroup>
<ISVoiceHuntGroupID>1</ISVoiceHuntGroupID>
</ISgetVoiceHuntGroup>
</request>
```

Response

```
<response>
<ISVoiceHuntGroups>
<ISVoiceHuntGroup>
<ISVoiceHuntGroupID>1</ISVoiceHuntGroupID>
<ISVoiceHuntGroupType>longest-idle</ISVoiceHuntGroupType>
<ISVoiceHuntGroupPilotNumber>200</ISVoiceHuntGroupPilotNumber>
<ISVoiceHuntGroupPilotPeerTag>200</ISVoiceHuntGroupPilotPeerTag>
<ISVoiceHuntGroupPilotPreference>0</ISVoiceHuntGroupPilotPreference>
<ISVoiceHuntGroupSecPilotNumber />
<ISVoiceHuntGroupSecPilotPeerTag>-1</ISVoiceHuntGroupSecPilotPeerTag>
<ISVoiceHuntGroupSecPilotPreference>0</ISVoiceHuntGroupSecPilotPreference>
<ISVoiceHuntGroupListSize>2</ISVoiceHuntGroupListSize>
<ISVoiceHuntGroupListNums>
<ISVoiceHuntGroupListNum>201</ISVoiceHuntGroupListNum>
<ISVoiceHuntGroupListNum>202</ISVoiceHuntGroupListNum>
</ISVoiceHuntGroupListNums>
<ISVoiceHuntGroupFinalNum />
<ISVoiceHuntGroupTimeout>180</ISVoiceHuntGroupTimeout>
<ISVoiceHuntGroupHops>2</ISVoiceHuntGroupHops>
</ISVoiceHuntGroup>
</ISVoiceHuntGroups>
</response>
```

ISgetPresenceGlobal

Use ISgetPresenceGlobal to retrieve configuration information and status for the presence engine in Cisco Unified CME.

Request

```
<request>
<ISgetPresenceGlobal />
</request>
```

Response

```
<response>
<ISPresenceGlobal>
<ISPresenceEnable>true</ISPresenceEnable>
<ISMode>cme</ISMode>
<ISAllowSub>true</ISAllowSub>
<ISAllowWatch>true</ISAllowWatch>
```

```
<ISMaxSubAllow>100</ISMaxSubAllow>
<ISSipUaPresenceStatus>false</ISSipUaPresenceStatus>
</ISPresenceGlobal>
</response>
```

Configure XML API

Note The following Cisco IOS commands that were previously used with the XML interface are no longer valid: **log password**, **xmltest**, **xmlschema**, and **xmlthread**.

Define XML Transport Parameters

To define the XML transport method and associated parameters, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ixi transport http**
5. **response size** *fragment-size*
6. **request outstanding** *number*
7. **request timeout** *seconds*
8. **no shutdown**
9. **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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the Cisco web browser user interface on the local Cisco Unified CME router.

	Command or Action	Purpose
Step 4	**ixi transport http** **Example:** `Router(config)# ixi transport http`	Specifies the XML transport method and enters XML-transport configuration mode. • **http**—HTTP transport.
Step 5	**response size** *fragment-size* **Example:** `Router(conf-xml-trans)# response size 8`	Sets the response buffer size. • *fragment-size*—Size of fragment in the response buffer, in kilobytes. Range is constrained by the transport type and platform. See the CLI help for the valid range of values.
Step 6	**request outstanding** *number* **Example:** `Router(conf-xml-trans)# request outstanding 2`	Sets the maximum number of outstanding requests allowed for the transport type. • *number*—Number of requests. Range is constrained by the transport type and platform. See the CLI help for the valid range of values.
Step 7	**request timeout** *seconds* **Example:** `Router(conf-xml-trans)# request timeout 30`	Sets the number of seconds to wait, while processing a request, before timing out. • *seconds*—Number of seconds. Range is 0 to 60.
Step 8	**no shutdown** **Example:** `Router(conf-xml-trans)# no shutdown`	Enables HTTP transport.
Step 9	**end** **Example:** `Router(config-xml-app)# end`	Returns to privileged EXEC mode.

Define XML Application Parameters

To set a response timeout for communication with the XML application that overrides the setting in transport configuration mode, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ixi application cme**
4. **response timeout** {**-1** | *seconds*}
5. **no shutdown**
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	**ixi application cme** **Example:** `Router(config)# ixi application cme`	Enters XML-application configuration mode for configuring Cisco IOS XML infrastructure parameters for the Cisco Unified CME application. **Note** This command defines URL of Cisco Unified CME XML server as `http://<routerIPaddress>/ios_xml_app/cme`.
Step 4	**response timeout** {**-1** | *seconds*} **Example:** `Router(config-xml-app)# response timeout 30`	Sets a timeout for responding to the XML application and overwrites the IXI transport level timeout. • **-1**—No application-specific timeout is specified. This is the default. • *seconds*—Length of timeout, in seconds. Range is 0 to 60.
Step 5	**no shutdown** **Example:** `Router(conf-xml-app)# no shutdown`	Enables XML communication with the application.
Step 6	**end** **Example:** `Router(config-xml-app)# end`	Returns to privileged EXEC mode.

Define Authentication for XML Access

To authenticate users for XML access, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **xml user** *user-name* **password** *password privilege-level*
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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**xml user** *user-name* **password** *password privilege-level* **Example:** `Router(config-telephony)# xml user user23 password 3Rs92uzQ 15`	Defines an authorized user. • *user-name*—Unique alphanumeric string that is authorized user name. Maximum length of string is 19 characters. • *password*—Alphanumeric string to use for access. Maximum length of string is 19 characters. • *privilege-level*—Level of access to Cisco IOS commands to be granted to this user. Only the commands with the same or a lower level can be executed via XML. Range is 0 (lowest) to 15 (highest).
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Define XML Event Table Parameters

The XML event table is an internal buffer that stores captured and time-stamped events, such as phones registering and unregistering and extension status. One event equals one entry in the table. To set the maximum number of events or entries that can be stored in the XML event table and the length of time that events are retained before they are deleted from the table, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **log table max-size** *number*
5. **log table retain-timer** *minutes*
6. **end**
7. **show fb-its-log**
8. **clear telephony-service xml-event-log**

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	**telephony-service** **Example:** `Router(config)#`	Enters telephony-service configuration mode.
Step 4	**log table max-size** *number* **Example:** `Router(config-telephony)# log table max-size 100`	Sets the number of entries in the XML event table. • *number*—Number of entries. Range is 0 to 1000. Default is 150.
Step 5	**log table retain-timer** *minutes* **Example:** `Router(config-telephony)# log table retain-timer 30`	Sets the number of minutes to retain entries in the event table before they are deleted. • *minutes*—Number of minutes. Range is 2 to 500. Default is 15.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.
Step 7	**show fb-its-log** **Example:** `Router# show fb-its-log`	Displays the event logs.
Step 8	**clear telephony-service xml-event-log** **Example:** `Router# clear telephony-service xml-event-log`	Clears XML event logs.

Troubleshooting the XML Interface

- Use the **debug cme-xml** command to view debug messages for the Cisco Unified CME XML interface.

Configuration Examples for XML API

Example for XML Transport Parameters

The following example selects HTTP as the XML transport method:

```
ip http server
ixi transport http
 response size 8
 request outstanding 2
 request timeout 30
 no shutdown
```

Example for XML Application Parameters

The following example sets the application response timeout to 30 seconds.

```
ixi application cme
 response timeout 30
 no shutdown
```

Example for XML Authentication

The following example selects HTTP as the XML transport method. It allows access for user23 with the password 3Rs92uzQ, and sets up access list 99 that accepts requests from the IP address 192.168.146.72.

```
ixi transport http
  ip http server
  !
  telephony-service
  xml user user23 password 3Rs92uzQ 15
```

Example for XML Event Table

The following example sets the maximum number of entries in the XML event table to 100 and the number of minutes to retain entries at 30:

```
telephony-service
   log table max-size 100
   log table retain-timer 30
```

Where to Go Next

For developer information on the XML API, see XML Provisioning Guide for Cisco CME/SRST.

Feature Information for XML API

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

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

Table 121: Feature Information for XML API

Feature Name	Cisco Unified CME Version	Feature Information
Call Blocking Based on Date and Time	4.0	The XML API was modified and is now provided through the Cisco IOS XML infrastructure. It supports all Cisco Unified CME features. The **log password**, **xmltest**, **xmlschema**, and **xmlthread** commands were made obsolete.
	3.0	The XML API was introduced.