Cisco Unified Communications Manager Express System Administrator Guide

September 27, 2007

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

Customer Order Number: OL-10663-02

CONTENTS

FEATURE MAP

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

Cisco Unified CME Features Roadmap

Last Updated: July 30, 2007

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 lists feature support for Cisco Unified CME versions. 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 the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists the 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.

Table 1 Supported Cisco Unified CME Features

Release	Feature Name	Feature Description	Where Documented
Cisco Unified CME 4.2			
4.2	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.	Configuring Extension Mobility
	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.	Configuring Interoperability with External Services

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	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.	Configuring Security
Cisco Unified CME 4.1			
4.1	Call Forward All Synchronization	When a user enables Call Forward All on a SIP phone using the CfwdAll soft key, 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 soft key to indicate that Call forward All is enabled.	Configuring Call Transfer and Forwarding
	Cisco Unified IP Phones	SCCP support was added for the following phone: • Cisco Unified IP Phone 7921G SIP support was added for the following phones: • 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 Communications Manager Express 4.1 Supported Firmware, Platforms, Memory, and Voice Products
	Directory Services	Local directory and local speed dial features are supported for SIP phones.	Configuring Directory Services
	Disabling SIP Supplementary Services for Call Forward and Call Transfer	You can disable 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. Disabling supplementary services is supported if all endpoints use SCCP or all endpoints use SIP.	Configuring Call Transfer and Forwarding
	KPML	Key Press Markup Language (KPML) reports 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.	Configuring Phones to Make Basic Calls
	Multi-Party Conferencing 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.	Configuring Conferencing

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Network Time Protocol	SIP phones registered to a Cisco Unified CME router can synchronize to a Network Time Protocol (NTP) server, known as the clock master.	Defining Network Parameters
	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.	Defining Network Parameters
	Presence with BLF Status	Presence supports 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.	Configuring Presence Service
	Restarting Phones	SIP phones can be quickly reset by using the **restart** command. Phones contact the TFTP server for updated configuration information and reregister without contacting the DHCP server.	Resetting and Restarting Phones
	Session Transport	TCP can be used as the transport protocol for supported SIP phones connected to Cisco Unified CME. Previously only UDP was supported.	Configuring Phones to Make Basic Calls
	SIP Dial Plans	Dial plans enable SIP phones to perform local digit collection and recognize dial patterns as user input is collected. After a pattern is recognized, the SIP phone sends an INVITE message to Cisco Unified CME to initiate the call.	Configuring Phones to Make Basic Calls
	Soft Keys	You can customize the display and order of soft keys that appear on individual SIP phones during the connected, hold, idle, and seized call states.	Customizing Soft Keys
	Translation Rules	SIP phones in a Cisco Unified CME system 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.	Configuring Dialing Plans
Cisco Unified CME 4.0(3)			
4.0(3)	AMWI	Cisco Unified IP Phone 7911 and Cisco Unified IP Phone 7931G can be configured to receive AMWI (Audible Message Line Indicator) and visual MWI notification from an external voice-messaging system.	Integrating Voice Mail
	Cisco Unified IP Phones	Support was added for the following phones: • Cisco Unified IP Phone 7906G • Cisco IP Unified IP Phone 7931G	Cisco Unified Communications Manager Express 4.0(3) Supported Firmware, Platforms, Memory, and Voice Products

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	DSS	DSS (Direct Station Select) 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.	Configuring Speed Dial
	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.	Creating Phone Configurations Using Extension Assigner
	Fax Relay	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.	Configuring Fax Relay
Cisco Unified CME 4.0(1)			
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.	Configuring Call Transfer and Forwarding
	Call Park	**Call park blocked per ephone**—Individual ephones can be blocked from parking calls at call-park slots. If a blocked ephone has a dedicated park slot, it can park calls at the dedicated park slot, but not at any other park slot. **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. The default is that hairpin call forwarding or transfer is used 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. Optional parameters include timeout intervals, after which the parked call can be automatically recalled to the parking phone or transferred to another number. **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.	Configuring Call Park

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Call Pickup	**Directed call pickup disable**—The **no service directed-pickup** command globally disables directed call pickup and changes the action of the PickUp soft key to invoke local group pickup rather than directed call pickup.	Configuring Call-Coverage Features
	Call Transfer	**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.	Configuring Call Transfer and Forwarding
	Cisco Unified IP Phones	Support was added 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.	Cisco Unified Communications Manager Express 4.0 Supported Firmware, Platforms, Memory, and Voice Products
	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.	Configuring Conferencing
	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.	Configuring Feature Access Codes
	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.	Configuring Headset Auto-Answer

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Hunt Groups	**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 soft key. 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 wildcard slots are configured for hunt groups and the agents' ephone-dns are authorized to join hunt groups. An agent joining a hunt group uses a wildcard slot, and an agent leaving a group relinquishes the slot so that another agent can use it. 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. No special configuration is required. **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. This text string can be used to indicate the name or purpose of the hunt group. A text string can be displayed on IP phones when all hunt-group members are logged out. This text string can be used to indicate where calls are being sent at that time; for example, to night service or voice mail. **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. **Longest-idle hunt group improvement**—A new command, the **from-ring** command, specifies that on-hook time stamps should be updated when a call rings an agent as well as when a call is answered by an agent.	Configuring Call-Coverage Features

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Hunt Groups	**Maximum number of agents** per hunt group has increased from 10 to 20. No special configuration is required. **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. **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.	Configuring Call-Coverage Features
	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.	Configuring Localization Support
	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.	Configuring Music on Hold

Table 1 Supported Cisco Unified CME Features (continued)

Release	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.	Configuring Call-Coverage Features
	Phone Support	**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 soft keys. 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.	Configuring Phones to Make Basic Calls
	Ring Tones	**Distinctive ringing**—An extension's ring patterns can be set to distinguish among internal, external, and feature calls.	Configuring Ring Tones
	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.	Configuring Security
	Soft keys	**Feature blocking**—The features associated with the following soft keys can be individually blocked per ephone: CFwdAll, Confrn, GpickUp, Park, PickUp, and Trnsfer. The soft key is not removed, but it does not function. **Soft-key control for hold state**—The soft keys that are available while a call is on hold can be modified. The NewCall and Resume soft keys are normally available when a phone has a call on hold, but a template can be applied to the phone to remove these soft keys.	Customizing Soft Keys
	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.	Configuring Speed Dial

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	System-Level Parameters	**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 operational again.	Configuring System-Level Parameters
	Templates	**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 soft keys 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** 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.	Creating Templates
	Video Support	**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.	Configuring Video Support for SCCP-Based Endpoints

Table 1 Supported Cisco Unified CME Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Voice Mail	**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.	Integrating Voice Mail
	XML Interface	**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.	Configuring the XML API

Cisco Unified CME Overview

Last Updated: July 31, 2007

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.

Contents

Information About Cisco Unified CME

To design and configure a Cisco Unified Communications Manager Express (Cisco Unified CME) system, you should understand the following concepts:

- Cisco Unified CME Overview, page 48
- Licenses, page 49
- PBX or Keyswitch Model, page 50

Cisco Unified CME Overview

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 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

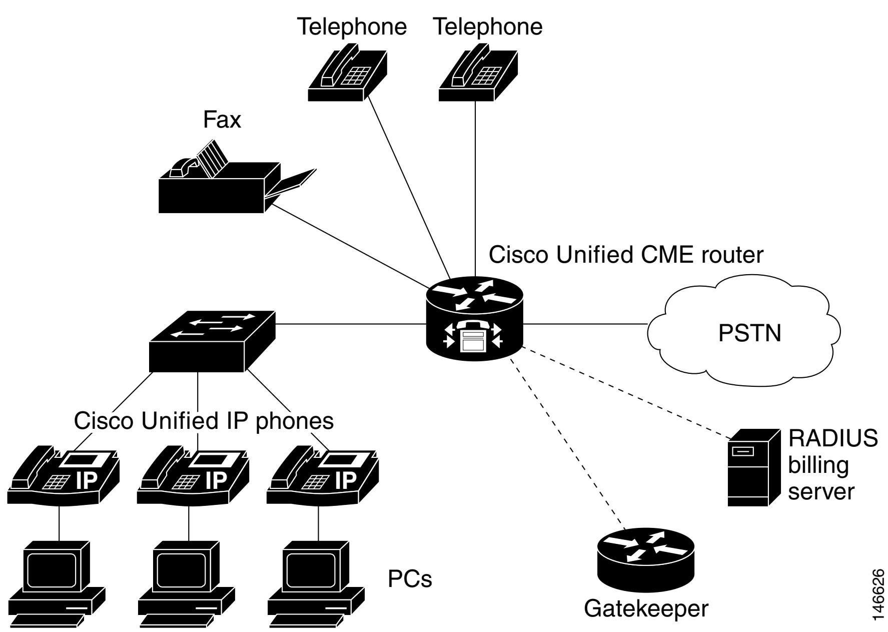
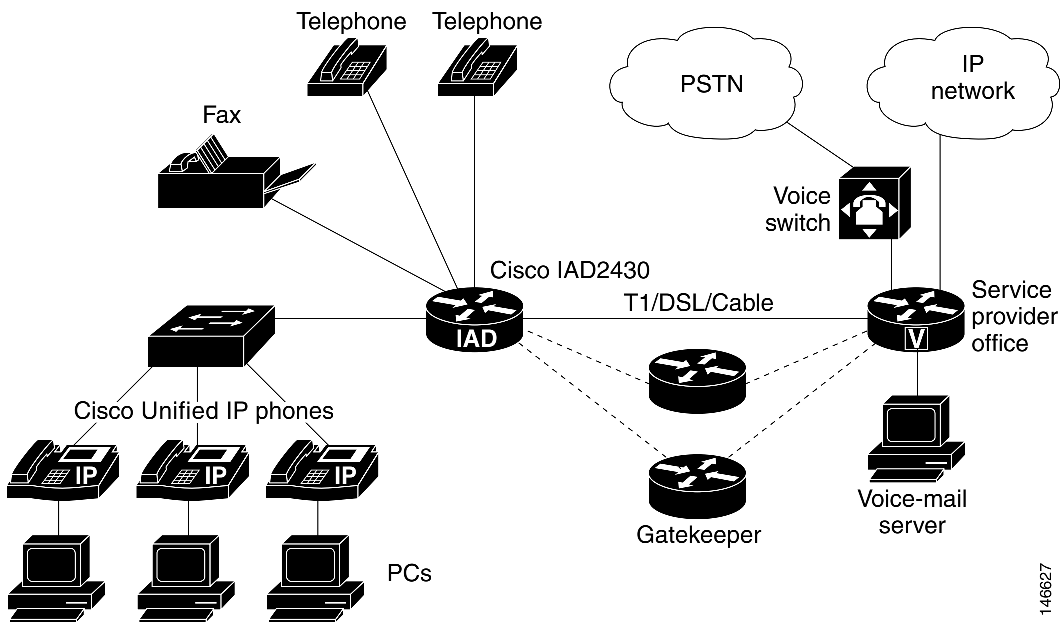


Figure 2 shows a branch office with several Cisco Unified IP phones connected to a Cisco IAD2430 series router with Cisco Unified CME. The Cisco IAD2430 router is connected to a multiservice router at a service provider office, which provides connection to the WAN and PSTN.

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.

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.

PBX or Keyswitch Model

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.

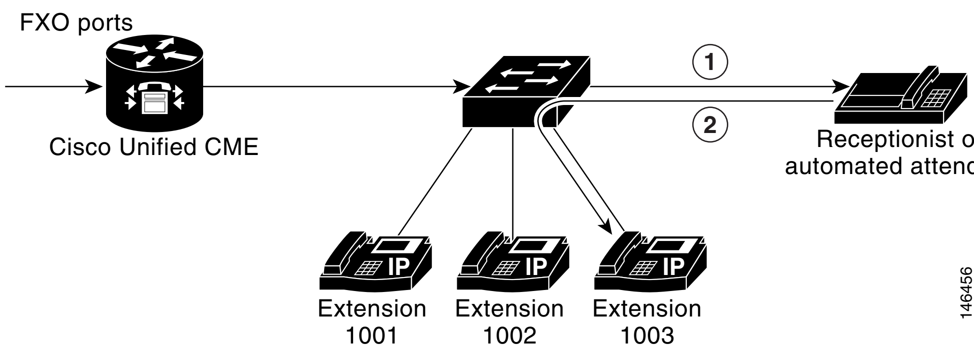
PBX Model

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 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 the "How to Configure Phones for a PBX System" section on page 177.

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.

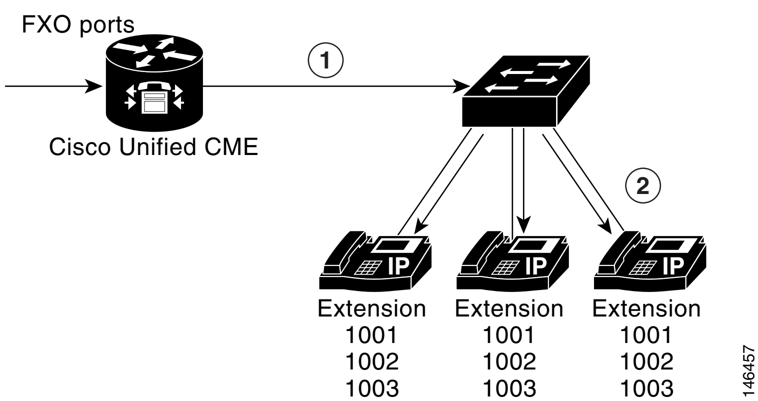
For example, a 3x3 keyswitch system has three PSTN lines shared across three telephones, such that all three PSTN lines appear on each of the three telephones. This permits an incoming call on any PSTN line to be directly answered by any telephone—without the aid of a receptionist, an auto-attendant 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 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 the "How to Configure Phones for a Key System" section on page 196.

Hybrid Model

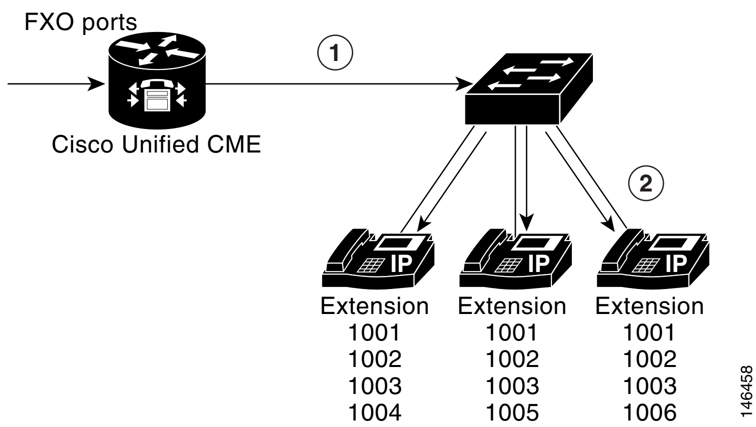
PBX and keyswitch configurations can be mixed on the same IP phone and can include both unique per-phone extensions for PBX-style calling and shared lines for keyswitch-style call operations. Single-line and dual-line directory numbers can be combined on the same phone.

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 and then add another, unique extension on each phone (Figure 5). 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



Where to Go Next

Before configuring Cisco Unified CME, see "Before You Begin" on page 57.

Additional References

The following sections provide references related to Cisco Unified CME.

Related Documents

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*

Related Topic	Document Title
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" part of the *Cisco IOS IP Addressing Services Configuration Guide*
Fax and modem configurations	• *Cisco IOS Fax and Modem Services over IP Application Guide*
FXS ports	**FXS Ports in H.323 Mode** • "Configuring Analog Voice Ports" section of the *Cisco IOS Voice Port Configuration Guide* • *Caller ID* **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
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 phones	• Cisco 7900 Series IP Phones • Cisco ATA 180 Series Analog Telephone Adaptors • Cisco IP Communicator
Phone documentation for Cisco Unified CME	• Quick Reference Cards and User Guides
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	• See links at *Cisco Unified CME Documentation Roadmap*
Tcl IVR and VoiceXML	• *Cisco IOS Tcl IVR and VoiceXML Application Guide - 12.3(14)T and later* • *Default Session Application Enhancements* • *Tcl IVR API Version 2.0 Programmer's Guide* • *Cisco VoiceXML 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*

Related Topic	Document Title
VSAs in call detail records (CDRs)	• *RADIUS VSA Voice Implementation Guide* • *Configuring Dynamic Prompts, Customizing Accounting Templates, and Directing AAA Requests for Voice Gateways*
XML	• *XML Provisioning Guide for Cisco CME/SRST* • *Cisco IP Phone Services Application Development Notes*

Related Websites

Related Topic	Title and Location
Cisco IOS configuration examples	Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html **Note** From the website, select a technology category and subsequent hierarchy of subcategories, and then click **Technical Documentation > Configuration Examples**.

MIBs

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

Technical Assistance

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

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

Before You Begin

Last Updated: July 31, 2007

This module describes general decisions that you should make before you configure Cisco Unified Communications Manager Express (Cisco Unified CME), information about tools for configuring Cisco Unified CME, and the work flow for creating or modifying a telephony configuration.

Contents

Prerequisites for Configuring Cisco Unified CME

- We recommend that you complete the worksheets to gather required site-specific information for the Cisco router to be configured. See the worksheet set at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_configuration_guide09186a0080759201.html#wp1007671.

Note Even though the worksheet set is for configuring a Typical (recommended) installation of an IP telephony system using Cisco Unified Communications Express - QCT, the information is required to create a telephony configuration using any of the configuration methods.

- 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 the "How to Install Cisco Voice Services Hardware" section on page 69.
- 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 the *Cisco Unified CME and Cisco IOS Software Compatibility Matrix*.
  - For a list of features for each Cisco IOS Software release, see the Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp.
  - For installation information, see the "How to Install Cisco IOS Software" section on page 72.
- 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 the "How to Configure VLANs on a Cisco Switch" section on page 73.

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

Before configuring Cisco Unified CME, you should understand the following concepts:

- System Design, page 59
- Configuration Methods Summary, page 60
- Cisco Unified Communications Express - QCT, page 62
- Cisco Unified CME GUI, page 64
- Workflow, page 64

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 the appropriate *Cisco CME Supported Firmware, Platforms, Memory, and Voice Products* document at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.
- 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 the appropriate *Cisco CME Supported Firmware, Platforms, Memory, and Voice Products* document at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.
- 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 165.

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 CME Solution Reference Network Design Guide* to help you understand the effect these factors have on your Cisco Unified CME implementation.

Configuration Methods Summary

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 2 compares the different methods for configuring Cisco Unified CME:

Table 2 Comparison of Configuration Methods for Cisco Unified CME

Configuration Method	Benefits	Restrictions
Cisco IOS command line interface For information about supported features, see Table 7. For information about using Cisco IOS commands, see the "Using Cisco IOS Commands to Create or Modify the Configuration" section on page 79.	• 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.

Table 2 Comparison of Configuration Methods for Cisco Unified CME (continued)

Configuration Method	Benefits	Restrictions
Cisco Unified Communications Express - QCT, page 62. For information about using Cisco Unified Communications Express - QCT, see the "Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration" section on page 80.	• Configuration wizard-like GUI. • Auto-discovers the hardware setup of the Cisco router. • Accept default values to quickly configure a typical basic IP telephony system or modify preconfigured values, enter data, and choose options to customize the configuration. • Generates commands for configuring an IP telephony system which can be uploaded to the Cisco router, along with the firmware files for all Cisco Unified IP phones to be connected to the Cisco router. • Configuration can be saved as template to be reused for additional systems. • Use for initial configuration including: basic information, such as VLANs, common DHCP pool, NTF servers, inbound and outbound destination numbers, and translation rules; and a subset of advanced features including paging, intercom, call park, hunt group, caller ID blocking, Class of Restriction, enabling video, and SIP truncking. • Can import user configuration data (names and extension numbers) from an external file. • Supports barcode-scanned input of MAC addresses and phone types.	• Factory-default configuration must be loaded in nonvolatile memory and in the running configuration of the Cisco router to be configured. **Note** Cisco Unified Communications Express - QCT can reset the running configuration on a router to factory-default. • Cannot be used to modify or maintain system configuration. • Configures limited subset of advanced features.
Cisco Unified CME GUI, page 64. For information about using the Cisco Unified CME GUI, see the "Using Cisco Unified CME GUI to Modify or Maintain Configuration" section on page 81.	• 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.

Cisco Unified Communications Express - QCT

Cisco Unified Communications Express - QCT 3.0 and later versions is an optional web-based application provided by Cisco Systems to simplify installation of a new stand-alone Cisco IP Communications Express (Cisco IPC Express). Cisco IPC Express is a complete communications solution for the small office or enterprise branch office installed on a single Cisco router running Cisco IOS IP Voice or higher. Cisco IPC Express includes Cisco Unified Communications Manager Express (Cisco Unified CME) for call processing and peripheral services like Cisco Unity Express voice mail, Automated Attendant (AA), and support for IP-phone based XML and Telephony Application Programming Interface (TAPI) applications. Although Cisco IPC Express can support up to 240 phone users, this tool is intended for installing the typical configuration for 50 or fewer users, on a Cisco Integrated Services Router Voice Bundle.

Cisco QCT does not configure advanced features including but not limited to Cisco Unity Express customized scripts, overlay-dn, and advanced ACD (Automatic Call Distributor). You will be required to use Cisco IOS commands, Cisco Unity Express GUI or command line interface (CLI), and other Cisco configuration tools to configure advanced features after using Cisco QCT. After you fill in the required fields, Cisco Unified Communications Express - QCT generates the corresponding commands and uploads the basic telephony configuration to your Cisco router.

Cisco Unified Communications Express - QCT supports auto-discovery of installed hardware, so you can deploy an IP telephony configuration without having detailed knowledge of the modules installed in the router. Cisco Unified Communications Express - QCT prompts for common parameters needed to configure a Cisco Integrated Services router to support a complete IP telephony solution as a private-branch-exchange (PBX) with direct-inward-dial extensions or as a square mode key system.

Before using Cisco Unified Communications Express - QCT, the factory-default configuration must be loaded in nonvolatile memory and in the running configuration of the Cisco router to be configured. You can use Cisco Unified Communications Express - QCT to restore the factory default configuration on router to be configured.

After using Cisco Unified Communications Express - QCT, you can add any feature not supported by Cisco Unified Communications Express - QCT to the configuration by using Cisco IOS commands.

Cisco Unified Communications Express - QCT cannot be used to perform routine additions and changes associated with employee turnover. You can use the Cisco Unified CME GUI or Cisco IOS commands to modify the basic telephony configuration generated by Cisco Unified Communications Express - QCT.

For information about rapid deployment of a brand new stand-alone Cisco IPC Express system, see the "Workflow" section on page 64. For information about using Cisco Unified Communications - QCT, see the "Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration" section on page 80.

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 world wide. 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 3 contains a list of the Cisco tools for deploying Cisco IPC Express.

Table 3 Cisco Tools for Deploying Cisco IPC Express

Tool Name	Description
Cisco Unified CME GUI, page 64	Cisco Unified CME GUI enables the user to configure a subset of optional system and phone features.
Cisco Unified Communications Express - Quick Configuration Tool (QCT)	Cisco Unified Communications Express - QCT is a web-based tool for automatically creating and downloading valid configuration files utilizing user-supplied values and/or preconfigured default parameters. This tool is the preferred method for configuring a new stand-alone Cisco IPC Express for 50 or fewer Cisco Unified CME users on a voice bundle.
Cisco IPC Express Quote-Builder	Cisco IPC Express Quote-Builder is an online application available to Cisco Systems partners to help them quickly identify recommended hardware configurations for Cisco IPC Express telephony systems based on the Cisco Integrated Services Router platform, which includes all versions of the Cisco 2800 and Cisco 3800 series routers.
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* at http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_documentation_roadmap09186a00803f3e19.html.	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.
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.

For information about using the Cisco Unified CME GUI, see the "Using Cisco Unified CME GUI to Modify or Maintain Configuration" section on page 81.

Workflow

This section contains the following topics:

Configuring Cisco Unified CME: Workflow

Table 4 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 4 Workflow for Creating or Modifying Basic Telephony Configuration

Task	Cisco Unified CME Configuration		Documentation
	New	Modify	
Install Cisco router and all recommended services hardware for Cisco Unified CME.	Required	Optional	Installing Hardware, page 70
Download recommended Cisco IOS IP Voice or higher image to flash memory in the router.	Optional	Optional	Installing Cisco IOS Software, page 72
Download recommended Cisco Unified CME software including phone firmware and GUI files.	Optional	Optional	Installing and Upgrading Cisco Unified CME Software, page 87
Configure separate virtual LANs (VLANS) for data and voice on the port switch.	Required[1]	—	Using Network Assistant to Configure a Cisco Catalyst Switch, page 73 or Using Cisco IOS Commands to Configure a Cisco Catalyst Switch, page 75 or Configuring VLANs on an Internal Cisco Ethernet Switching Module, page 77
• 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[1]	Optional	Defining Network Parameters, page 109
• 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[1]	Optional	Configuring System-Level Parameters, page 137
• 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[1]	Optional	Configuring Phones to Make Basic Calls, page 165
Connect to PSTN.	Required[1]	—	Configuring Dialing Plans, page 287

Table 4 Workflow for Creating or Modifying Basic Telephony Configuration (continued)

Task	Cisco Unified CME Configuration		Documentation
	New	Modify	
Install system- and user-defined files for localization of phones.	Optional[2]	Optional	Configuring Localization Support, page 307
Enable call detail records (CDRs) for collecting accounting data.	Optional	Optional	*RADIUS VSA Voice Implementation Guide*

1. Can be configured by using Cisco Unified Communications Express - QCT to generate a basic telephony configuration for Cisco Unified CME. For information, see the "Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration" section on page 80.
2. Required for certain Cisco Unified IP phones such as the Cisco Unified IP Phone 7911, 7941, 7961, 7970, and 7971. See documentation for more information.

Table 5 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 37.

Table 5 Workflow for Adding Features in Cisco Unified CME

Task	Documentation
Configure transcoding to support conferencing, call transferring and forwarding, MoH, and Cisco Unity Express.[1]	Configuring Transcoding Resources, page 323
Enable the graphical user interface in Cisco Unified CME.[1]	Enabling the GUI, page 359
Configure support for voice mail.[1,2]	Integrating Voice Mail, page 375
Configure interoperability with Cisco Unified CCX.	Configuring Interoperability with External Services, page 965
Configure authentication support.	Configuring Security, page 409

Table 5 Workflow for Adding Features in Cisco Unified CME (continued)

Task	Documentation
Add features. **Note** Cisco Unified Communications Express - QCT can configure only a subset of features. You must use Cisco IOS commands to add other features. • Call Blocking • Call-Coverage Features, including: – Call Hunt – Call Pickup[1] – Call Waiting – Callback Busy Subscriber – Hunt Groups[1] – Night Service – Overlaid Ephone-dns • Call Park[1] • Call Transfer and Forwarding • Caller ID Blocking[1] • Conferencing • Intercom Lines[1] • Music on Hold (MoH) • Paging[1]	• Configuring Automatic Line Selection, page 479 • Configuring Call Blocking, page 485 • Configuring Call-Coverage Features, page 581 • Configuring Call Park, page 503 • Configuring Call Transfer and Forwarding, page 517 • Configuring Caller ID Blocking, page 657 • Configuring Conferencing, page 665 • Configuring Directory Services, page 707 • Configuring Do Not Disturb, page 727 • Configuring Extension Mobility, page 763 • Configuring Feature Access Codes, page 775 • Configuring Headset Auto-Answer, page 791 • Configuring Intercom Lines, page 799 • Configuring Loopback Call Routing, page 809 • Configuring Music on Hold, page 817 • Configuring Paging, page 831 • Configuring Presence Service, page 843 • Configuring Ring Tones, page 865 • Customizing Soft Keys, page 875 • Configuring Speed Dial, page 893
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	Modifying Cisco Unified IP Phone Options, page 939
Configure video support.[1]	Configuring Video Support for SCCP-Based Endpoints, page 913
Configure Cisco Unified CME as SRST Fallback.	Configuring SRST Fallback Support, page 989

1. Can be configured by using Cisco Unified Communications Express - QCT to generate a basic telephony configuration for Cisco Unified CME. For information, see the "Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration" section on page 80.

2. Cisco Unified Communications Express - QCT configures support for Cisco Unity Express only. Support for integrating with other voice-mail systems must be configured by using Cisco IOS commands.

Using Cisco Unified Communications Express- QCT to Configure Cisco IPC Express: Workflow

Table 6 lists the tasks for installing and configuring a brand new stand-alone Cisco IPC Express system, including Cisco Unified CME and Cisco Unity Express voice mail, in the suggested order in which the tasks are to be performed and including links to modules in this guide that support each task.

For information about modifying the configuration of an existing Cisco IPC Express system, see "Configuring Cisco Unified CME: Workflow" section on page 64.

Table 6 Workflow for Using Cisco Unified Communications Express - QCT to Configure Cisco IPC Express

Task	Documentation
Install Cisco router and all recommended services hardware for Cisco Unified CME.	Installing Hardware, page 70
Download recommended Cisco IOS IP Voice or higher image to flash memory in the router.	Installing Cisco IOS Software, page 72
Download recommended Cisco Unified CME software including phone firmware and GUI files.	Installing and Upgrading Cisco Unified CME Software, page 87
Use Cisco Unified Communications Express - QCT to generate and upload a basic telephony configuration for Cisco IPC Express.	Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration, page 80
Install system- and user-defined files for localization of phones.	Configuring Localization Support, page 307
Add features. **Note** Cisco Unified Communications Express - QCT can configure only a subset of features. You must use Cisco IOS commands to add other features.	• Configuring Automatic Line Selection, page 479 • Configuring Call Blocking, page 485 • Configuring Call Transfer and Forwarding, page 517 • Configuring Conferencing, page 665 • Configuring Directory Services, page 707 • Configuring Do Not Disturb, page 727 • Configuring Extension Mobility, page 763 • Configuring Feature Access Codes, page 775 • Configuring Headset Auto-Answer, page 791 • Configuring Loopback Call Routing, page 809 • Configuring Music on Hold, page 817 • Configuring Presence Service, page 843 • Configuring Ring Tones, page 865 • Customizing Soft Keys, page 875 • Configuring Speed Dial, page 893
Configure authentication support.	Configuring Security, page 409

Table 6 Workflow for Using Cisco Unified Communications Express - QCT to Configure Cisco IPC Express

Task	Documentation
Configure conferencing features, including: • Call hunt • Call waiting • Callback busy subscriber • Night service • Overlaid Ephone-dns	Configuring Conferencing, page 665
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	Modifying Cisco Unified IP Phone Options, page 939
Configure support for interoperability with Cisco Unified CCX.	Configuring Interoperability with External Services, page 965
Configure Cisco Unified CME as fallback.	Configuring SRST Fallback Support, page 989

How to 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.

Prerequisites

- Cisco router and all recommended hardware for Cisco Unified CME, and if required, Cisco Unity Express, is ordered and delivered, or is already onsite. To determine the recommended hardware configuration to support your telephony system requirements, see the Cisco IPC Express Quote-Builder online tool.

Installing Hardware

To install the Cisco router and voice services hardware, perform the following steps.

SUMMARY STEPS

1. Install the Cisco router on the network.
2. Connect to the Cisco router.
3. Use the **show version** or **show flash** command to check the amount of memory installed in the router.
4. Identify DRAM and flash memory requirements.
5. Install or upgrade system memory.
6. Install Cisco voice services hardware.
7. Disable Smartinit and allocate ten percent of the total memory to Input/Output (I/O) memory.

DETAILED STEPS

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. For more information on cabling, and details about how to connect a terminal to the console port or the AUX port, see *Cabling Guide for Console and Aux Ports on Cisco Routers*.

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 s**how 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.

Example:

```
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 *Cisco Unified CME Supported Firmware, Platforms, Memory, and Voice Products* for the Cisco Unified CME version you are using at: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html

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
```

How to 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.

Prerequisites

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

Installing Cisco IOS Software

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.

SUMMARY STEPS

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

DETAILED STEPS

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

Example:

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

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

Step 3 To download and extract the recommended Cisco IOS IP Voice or higher image to flash memory in the router. See *Copying Images from a Network Server to flash Memory*.

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 the "Installing Cisco Unified CME Software" section on page 92.
- If you want to use Cisco Unified Communications Express - QCT to generate and upload a basic telephony configuration, see the "Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration" section on page 80.
- If you are installing a new stand-alone Cisco Unified CME system and you are *not* using Cisco Unified Communications Express - QCT to generate and upload a basic telephony configuration, see the "How to Configure VLANs on a Cisco Switch" section on page 73.

How to Configure VLANs on a Cisco Switch

Note If you used or are using Cisco Unified Communications express - QCT to configure Cisco Unified CME or a Cisco IPC Express system, skip this task and see "Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration" section on page 80.

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.

- Using Network Assistant to Configure a Cisco Catalyst Switch, page 73
- Using Cisco IOS Commands to Configure a Cisco Catalyst Switch, page 75
- Configuring VLANs on an Internal Cisco Ethernet Switching Module, page 77

Using Network Assistant to Configure a Cisco Catalyst Switch

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.

Prerequisites

- 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* at:
  http://www.cisco.com/en/US/products/ps5931/prod_release_notes_list.html.

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.

  For more information on cabling and details about how to connect a management station or modem to the console port, see "Connecting to the Console Port" at:
  http://cisco.com/en/US/products/hw/switches/ps597/products_installation_and_configuration_guide_chapter09186a008007ef5f.html#xtocid14.

SUMMARY STEPS

1. Install, launch, and connect Cisco Network Assistant.
2. Use Network assistant to enable two VLANs on the switch port, configure a trunk between the Cisco Unified CME router and the switch, and configure Cisco IOS Quality-of-Service (QoS).

DETAILED STEPS

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).

What to Do Next

See the "Using Cisco IOS Commands to Create or Modify the Configuration" section on page 79.

Using Cisco IOS Commands to Configure a Cisco Catalyst Switch

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.

Prerequisites

- 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.

  For more information on cabling and details about how to connect a management station or modem to the console port, see "Connecting to the Console Port" at: http://cisco.com/en/US/products/hw/switches/ps597/products_installation_and_configuration_guide_chapter09186a008007ef5f.html#xtocid14.

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.
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.

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

What to Do Next

See the "Using Cisco IOS Commands to Create or Modify the Configuration" section on page 79.

Configuring VLANs on an 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.

Prerequisites

- 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.
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 the "Using Cisco IOS Commands to Create or Modify the Configuration" section on page 79.

How to Configure Cisco Unified CME

This section contains the following tasks:

- Using Cisco IOS Commands to Create or Modify the Configuration, page 79
- Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration, page 80
- Using Cisco Unified CME GUI to Modify or Maintain Configuration, page 81

Using Cisco IOS Commands to Create or Modify the Configuration

Note For information about the Cisco IOS Command-Line Interface (CLI) and command modes, see Using Cisco IOS Software.

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.
- To establish a physical console connection, attach a terminal or PC running terminal emulation to the console port of the router. For more information on cabling, and details about how to connect a terminal to the console port or the AUX port, see Cabling Guide for Console and Aux Ports on Cisco Routers.

  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
- We recommend that you complete the worksheets to gather required site-specific information for the Cisco router to be configured. See the worksheet set at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_configuration_guide09186a0080759201.html#wp1007671.

Note Even though the worksheet set is for configuring a Typical (recommended) installation of an IP telephony system using Cisco Unified Communications Express - QCT, the information is required to create an initial configuration using any of the configuration methods.

What to Do Next

For step-by-step procedures for configuring Cisco Unified CME using Cisco IOS commands, see the *Cisco Unified CME System Administrator Guide*.

Using Cisco Unified Communications Express - QCT to Generate a Telephony Configuration

To u se Cisco Unified Communications Express - QCT to generate a basic telephony configuration for a PBX or Square Mode (key system) system, with or without Cisco Unity Express, or to reset the configuration of a Cisco router to factory default, see the *Cisco Unified Communications Express - QCT User Guide*.

Prerequisites

- Your IP network is operational and you can access Cisco web.
- A PC with Microsoft® Internet Explorer 5.5 or a later version is connected, using a serial cable, to the console port of Cisco router to be configured. If you need assistance in connecting your PC to your router's console port, refer to the Install and Upgrade Guide for the Cisco router.
- The Block Pop-up Windows feature for Microsoft® Internet Explorer must be disabled.
- You must be a member of Administrators group under User Account settings for your PC.
- You must have a valid Cisco CCO account.
- The factory-default configuration is loaded in nonvolatile memory and in the running configuration of the Cisco router to be configured.

Note Cisco Unified Communications Express - QCT can be used to restore the factory default configuration on router to be configured.

- If you are using Cisco Unified Communications Express - QCT to upload firmware files for Cisco Unified IP phones after uploading the generated configuration, all Cisco firmware files to be uploaded must be installed in the folder named Phoneloads, within the local folder in which Cisco Unified Communications Express - QCT is installed.
- *Worksheets for Cisco Unified Communications Express - QCT* are complete with required site-specific information for the Cisco router to be configured.

Restrictions

- Cisco Unified Communications Express - QCT cannot be used to perform routine additions and changes associated with employee turnover.
- Cisco Unified Communications Express - QCT can configure only a subset of features of Cisco Unified CME and generate the basic telephony configuration.

What to Do Next

After using Cisco Unified Communications Express - QCT to generate a basic telephony configuration, you can skip the following modules in the *Cisco Unified CME System Administrator Guide* when you use Cisco IOS commands to add features to the initial configuration:

- Defining Network Parameters
- Configuring System-Level Parameters
- Configuring Phones to Make Basic Calls

- Creating Phone Configurations Using Extension Assigner
- Configuring Dialing Plans
- Adding Features, but only for the following:
  - Configuring Call Blocking
  - Configuring Call Park
  - Configuring Call Transfer and Forwarding
  - Configuring Call-Coverage Features
  - Configuring Caller ID Blocking
  - Configuring Conferencing
  - Configuring Intercom Lines
  - Configuring Music on Hold
  - Configuring Paging
- Enabling the GUI
- Configuring Voice-Mail Support (for Cisco Unity Express only). To add support Cisco Unity or other voice-mail systems, you must use Cisco IOS commands to modify the configuration.

Using Cisco Unified CME GUI to Modify or Maintain Configuration

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 "Installing and Upgrading Cisco Unified CME Software" on page 87.
- Cisco Unified CME GUI must be enabled. For information, see "Enabling the GUI" on page 359.

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.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Summary

Table 7 contains a list of 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 37.

Table 7 Parameters and Features Supported by Cisco IOS Commands

Parameters and Features	Where to Find Configuration Information
Cisco Unified CME Software	
Installing and upgrading software, including: • Cisco Unified CME • Cisco Unified CME GUI • Firmware files for Cisco Unified IP phones	Installing and Upgrading Cisco Unified CME Software
Basic Configuration	
• Enabling Calls in Your VoIP Network • Defining DHCP • Setting Network Time Protocol • Configuring DTMF Relay for H.323 Networks in Multisite Installations • Configuring SIP Trunk Support • Changing the TFTP Address on a DHCP Server • Enabling OOD-R	Defining Network Parameters
• Configuring Bulk Registration • Setting Up Cisco Unified CME • Setting Date and Time Parameters • Blocking Automatic Registration • Defining Alternate Location and Type of Configuration Files • Changing Defaults for Time Outs • Configuring a Redundant Router	Configuring System-Level Parameters
• Creating Directory Numbers, Assigning Directory Numbers to Phones • Creating Phone Configurations Using Extension Assigner • Generating Configuration Files for Phones • Resetting and Restarting Phones	Configuring Phones to Make Basic Calls
Connecting to PSTN	
• Dial-plan patterns • Translation rules and profiles • Secondary dial tones	Configuring Dialing Plans

Table 7 Parameters and Features Supported by Cisco IOS Commands

Parameters and Features	Where to Find Configuration Information
Transcoding Support	
• DSP farms • NMs or NM farms • Transcoding sessions	Configuring Transcoding Resources.
Localization Support	
• Use locale • Network locale	Configuring Localization Support.
Cisco Unified CME GUI	Enabling the GUI
Features	
• Automatic line selection • Call blocking • Call park • Call transfer and forwarding • Caller ID blocking • Conferencing • Directory services • Do Not Disturb (DND) • Feature Access Codes (FAC) • Headset auto-answer • Intercom lines • Loopback call routing • Music on Hold (MOH) • Paging • Presence service • Ring tones • Soft keys • Speed dial	Adding Features
• Call hunt • Call pickup • Call waiting • Callback busy subscriber • Hunt groups • Night service • Overlaid Ephone-dns	Configuring Call-Coverage Features.

Table 7 Parameters and Features Supported by Cisco IOS Commands

Parameters and Features	Where to Find Configuration Information
Authentication Support	
• Phone authentication startup messages • CTL file • CTL client and provider • MIC root certificate	Configuring Security.
Phone Options	
• 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	Modifying Cisco Unified IP Phone Options.
Video Support	Configuring Video Support for SCCP-Based Endpoints
Voice-Mail Support	
• Cisco Unity Connection • Cisco Unity Express • Cisco Unity • DTMF integration for legacy voice-mail applications • Mailbox selection policy • RFC 2833 Dual Tone Multifrequency (DTMF) MTP Passthrough • MWI	Integrating Voice Mail.
Cisco Unified CME as SRST fallback	Configuring SRST Fallback Support.

Installing and Upgrading Cisco Unified CME Software

Last Updated: July 13, 2007

This chapter explains how to install Cisco Unified Communications Manager Express (Cisco Unified CME) software and how to upgrade phone firmware for Cisco Unified IP phones.

Contents

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 the "How to Install Cisco Voice Services Hardware" section on page 69.

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 the *Cisco Unified CME and Cisco IOS Software Compatibility Matrix*. For installation information, see the "How to Install Cisco IOS Software" section on page 71.

Information About 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 the "Installing Cisco Unified CME Software" section on page 92.

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 the "Installing Cisco Unified CME Software" section on page 92.

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, 796GE, 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 8 contains firmware-naming convention examples, in alphabetical order:

Table 8 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
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 *Cisco CME Supported Firmware, Platforms, Memory, and Voice Products* document at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

For information about installing firmware files, see the "Installing Cisco Unified CME Software" section on page 92.

For information about configuring Cisco Unified CME for upgrading between versions or converting between SCCP and SIP, see the "How to Install and Upgrade Cisco Unified CME Software" section on page 92.

IXML 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 the "Installing Cisco Unified CME Software" section on page 92.

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 the "Installing Cisco Unified CME Software" section on page 92.

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 the appropriate *Cisco CME B-ACD and TCL Call-Handling Applications* document at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

For information about installing TcL script file or an archive, see "Installing Cisco Unified CME Software" on page 92.

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 the TSP documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_programming_reference_guide09186a00801c5f9c.html.

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:

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* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.
cme-b-acd...	Files required for Cisco Unified CME B-ACD service.

Cisco Unified Communications Express - Quick Configuration Tool

Cisco Unified Communications Express - Quick Configuration Tool (Cisco Unified Communications Express - QCT) 3.0 or a later version is a GUI application provided for Cisco Partners and Resellers designed to simplify and expedite the configuration of Cisco Unified Communications Manager Express (Cisco Unified CME) and Cisco Unity Express by reducing the number of Cisco IOS commands with which the user must be familiar in order to deploy a Cisco Unified Communications Express telephony system.

Use Cisco Unified Communications Express - QCT to set up a simple, typical basic PBX or key system telephony configuration of 50 or fewer IP phone users on any Cisco Unified CME supported Cisco Integrated Services Router platform, including the Cisco 2800 and the Cisco 3800 product families. In addition, Cisco Unified Communications Express - QCT recognizes any Advanced Integrated Module (AIM) or NM-CUE module installed in the router, thus providing voice-mail and Auto Attendant (AA) capability to the Cisco Unified CME system.

After all the necessary information is entered, Cisco Unified Communications Express - QCT generates all of the required configuration commands which you can upload to the Cisco router to be configured or save as a template file to use to configure additional systems with similar system parameters.

For information about installing and using Cisco Unified Communications Express - QCT, see the *Cisco Unified Communications Express - QCT User Guide.*

How to Install and Upgrade Cisco Unified CME Software

This section contains the following procedures:

- Installing Cisco Unified CME Software, page 92 (required)
- SCCP: Upgrading or Downgrading Phone Firmware Between Versions, page 94 (required)
- SIP: Upgrading or Downgrading Phone Firmware Between Versions, page 95 (required)
- SCCP: Converting Phone Firmware to SIP, page 99 (required)
- SIP: Converting Phone to SCCP, page 102 (required)
- SCCP: Verifying the Phone Firmware Version on an IP Phone, page 106 (optional)
- Troubleshooting Tips, page 106 (optional)

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.

Installing Cisco Unified CME Software

To install Cisco Unified CME in flash memory, perform the following steps.

SUMMARY STEPS

1. Go to Software Download site.
2. Download archive.
3. Extract files to be downloaded.
4. Use the **copy** or **archive tar** command to copy file to flash memory.
5. Use the **show flash:** command to list files in flash memory.

DETAILED STEPS

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
```

What to Do Next

- If you installed Cisco Unified CME software and Cisco Unified CME is *not* configured on your router, see "Defining Network Parameters" on page 109.
- 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 the "SCCP: Upgrading or Downgrading Phone Firmware Between Versions" section on page 94.
- 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 the "SIP: Upgrading or Downgrading Phone Firmware Between Versions" section on page 95.
- 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 the "SCCP: Converting Phone Firmware to SIP" section on page 99.
- 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 the "SCCP: Converting Phone Firmware to SIP" section on page 99.
- 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 the "SIP: Converting Phone to SCCP" section on page 102.

SCCP: Upgrading or Downgrading Phone Firmware Between Versions

To downgrade or upgrade firmware versions on a Cisco Unified IP phone running SCCP, perform the following steps.

Prerequisites

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 the "Installing Cisco Unified CME Software" section on page 92.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **load** *phone-type firmware-file*
5. **create cnf**
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	**tftp-server flash:** *file-name* **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`	Enables TFTP file sharing for new phone firmware files. • A separate **tftp-server flash** command is required for each firmware file to be downloaded to this phone.
Step 4	**telephony service** **Example:** `Router(config)# telephony service`	Enters telephone-service configuration mode.

	Command or Action	Purpose
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.
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 configuration mode and enters privileged EXEC mode.

What to Do Next

- If the Cisco Unified IP phone to be upgraded is not configured in Cisco Unified CME, see "How to Configure Phones for a PBX System" on page 177.
- 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 "Resetting and Restarting Phones" on page 277.

SIP: Upgrading or Downgrading Phone Firmware Between Versions

To upgrade or downgrade phone firmware for Cisco Unified IP phones running SIP between versions, perform the steps in this section.

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.

Prerequisites

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 the "Installing Cisco Unified CME Software" section on page 92.

Restrictions

- 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 the phone firmware upgrade matrix at: http://www.cisco.com/en/US/products/sw/voicesw/ps4967/prod_installation_guides_list.html.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode cme**
5. **load** *phone-type firmware-file*
6. **upgrade**
7. Repeat Steps 5 and 6.
8. **file text**
9. **create profile**
10. **exit**
11. **voice register 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.

	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	**`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 previous two steps. **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.
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.

	Command or Action	Purpose
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.

Examples

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 "How to Configure Phones for a PBX System" on page 177.
- 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 "Resetting and Restarting Phones" on page 277.

SCCP: Converting Phone Firmware to SIP

To upgrade the phone firmware for a particular phone from SCCP to SIP, follow the steps in this task.

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 the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.

Prerequisites

- 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 the "Installing Cisco Unified CME Software" section on page 92.
- 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 previous two steps.
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.
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.

	Command or Action	Purpose
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 previous two steps **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.
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.

Examples

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 "How to Configure Phones for a PBX System" on page 177.
- If the Cisco Unified IP phones to be upgraded are already configured in Cisco Unified CME, see "Resetting and Restarting Phones" on page 277.

SIP: Converting Phone to SCCP

To upgrade the phone firmware for a particular phone from SIP to SCCP, follow the steps in this task.

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 "How to Configure Phones for a PBX System" on page 177.

Prerequisites

- 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 the "Installing Cisco Unified CME Software" section on page 92.
- 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 the "SIP: Upgrading or Downgrading Phone Firmware Between Versions" section on page 95.

Removing a 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.
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 change will apply.
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.

Generating an SCCP XML Configuration File for Upgrading 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 flash** *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.
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 flash:`** *`file-name`* **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`	Enables TFTP file sharing for new phone firmware files. • A separate **tftp-server flash** command is required for each firmware file to be downloaded to this phone.
Step 6	**`telephony service`** **Example:** `Router(config)# telephony service`	Enters telephone-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 to be associated with the specified IP phone type. • Do not use the .sbin or .loads file extension except for Cisco ATA and Cisco Unified IP Phone 7905 and 7912

	Command or Action	Purpose
Step 8	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds XML configuration files required for SCCP phones.
Step 9	**end** **Example:** `Router(config-telephony)# end`	Exits configuration mode and enters privileged EXEC mode.

Examples

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)# 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)# exit
Router(config)# no voice register pool 1
Router(config-register-pool)# exit
Router(config)# voice 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 "How to Configure Phones for a PBX System" on page 177.
- If the Cisco Unified IP phones to be upgraded are already configured in Cisco Unified CME, see "Resetting and Restarting Phones" on page 277.

SCCP: Verifying the Phone Firmware Version on an IP Phone

To verify which version firmware is on an IP phone, perform the following steps.

SUMMARY STEPS

1. **show flash:**
2. **show ephone phone-load**

DETAILED STEPS

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

Use the **debug tftp event** command to troubleshoot an attempt to upgrade or convert Cisco phone firmware files for SIP phones. The following sample from the **debug tftp event** command shows how the Cisco phone firmware for a Cisco Unified IP Phone 7940G is upgraded from SCCP 5.X to SIP 6.3. The configuration profiles are downloaded when a phone is rebooted or reset.

```
Router# debug tftp event
…
Router(config)#telephony-service
Router(config-telephony)#no create cnf
CNF files deleted
Router(config-telephony)#voice register global
Router(config-register-global)#load 7960 P0S3-06-3-00
Router(config-register-global)#upgrade
Router(config-register-global)#create profile
Router(config-register-global)#
*May 6 17:37:03.737: %IPPHONE-6-UNREGISTER_NORMAL: ephone-1:SEP000ED7DF7932 IP:1.5.49.84
Socket:4
DeviceType:Phone has unregistered normally.
*May 6 17:37:35.949: TFTP: Looking for OS79XX.TXT
*May 6 17:37:36.413: TFTP: Opened system:/cme/sipphone/OS79XX.TXT, fd 4, size 13 for
process 81
```

```
*May 6 17:37:36.413: TFTP: Finished system:/cme/sipphone/OS79XX.TXT, time 00:00:00 for
process 81
*May 6 17:37:40.533: TFTP: Looking for P0S3-06-3-00.sbn
*May 6 17:37:40.541: TFTP: Opened flash:P0S3-06-3-00.sbn, fd 4, size 487198 for process 81
*May 6 17:37:48.225: TFTP: Finished flash:P0S3-06-3-00.sbn, time 00:00:07 for process 81
*May 6 17:40:26.925: TFTP: Looking for OS79XX.TXT
*May 6 17:40:26.925: TFTP: Opened system:/cme/sipphone/OS79XX.TXT, fd 4, size 13 for
process 81
*May 6 17:40:26.925: TFTP: Finished system:/cme/sipphone/OS79XX.TXT, time 00:00:00 for
process 81
*May 6 17:40:26.929: TFTP: Looking for SIPDefault.cnf
*May 6 17:40:26.929: TFTP: Opened system:/cme/sipphone/SIPDefault.cnf, fd 4, size 1558 for
process 81
*May 6 17:40:26.937: TFTP: Finished system:/cme/sipphone/SIPDefault.cnf, time 00:00:00 for
process 81
*May 6 17:40:27.053: TFTP: Looking for SIP000ED7DF7932.cnf
*May 6 17:40:27.053: TFTP: Opened system:/cme/sipphone/SIP000ED7DF7932.cnf, fd 4, size 789
for process 81
*May 6 17:40:27.057: TFTP: Finished system:/cme/sipphone/SIP000ED7DF7932.cnf, time
00:00:00 for process 81
```

The following sample from the **debug tftp event** command shows how the Cisco phone firmware for a Cisco Unified IP Phone 7940G is upgraded from SIP 6.3 to SIP 7.0 after the phone is rebooted or reset:

```
Router# debug tftp event
…
Router(config-register-global)#load 7960 P003-07-4-00
Router(config-register-global)#upgrade
Router(config-register-global)#load 7960 P0S3-07-4-00
Router(config-register-global)#create profile
Router(config-register-global)#end
Router-2012#
*May 6 17:42:35.581: TFTP: Looking for OS79XX.TXT
*May 6 17:42:35.585: TFTP: Opened system:/cme/sipphone/OS79XX.TXT, fd 5, size 13 for
process 81
*May 6 17:42:35.585: TFTP: Finished system:/cme/sipphone/OS79XX.TXT, time 00:00:00 for
process 81
*May 6 17:42:35.969: TFTP: Looking for P003-07-4-00.sbn
*May 6 17:42:35.977: TFTP: Opened slot0:P003-07-4-00.sbn, fd 5, size 129876 for process 81
*May 6 17:42:37.937: TFTP: Finished slot0:P003-07-4-00.sbn, time 00:00:01 for process 81
*May 6 17:44:31.037: TFTP: Looking for CTLSEP000ED7DF7932.tlv
*May 6 17:44:31.057: TFTP: Looking for SEP000ED7DF7932.cnf.xml
*May 6 17:44:31.089: TFTP: Looking for SIP000ED7DF7932.cnf
*May 6 17:44:31.089: TFTP: Opened system:/cme/sipphone/SIP000ED7DF7932.cnf, fd 5, size 789
for process 81
*May 6 17:44:31.089: TFTP: Finished system:/cme/sipphone/SIP000ED7DF7932.cnf, time
00:00:00 for process 81
*May 6 17:44:31.125: TFTP: Looking for P0S3-07-4-00.loads
*May 6 17:44:31.133: TFTP: Opened slot0:P0S3-07-4-00.loads, fd 5, size 461 for process 81
*May 6 17:44:31.141: TFTP: Finished slot0:P0S3-07-4-00.loads, time 00:00:00 for process 81
*May 6 17:44:31.673: TFTP: Looking for P0S3-07-4-00.sb2
*May 6 17:44:31.681: TFTP: Opened slot0:P0S3-07-4-00.sb2, fd 5, size 592626 for process 81
*May 6 17:44:33.989: TFTP: Finished slot0:P0S3-07-4-00.sb2, time 00:00:02 for process 81
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	• *Cisco Unified CME Command Reference* • *Cisco Unified CME Documentation Roadmap* • *Cisco Unified Communications Express - QCT User Guide*
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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Defining Network Parameters

Last Updated: September 27, 2007

This chapter describes how to define parameters that enable Cisco Unified Communications Manager Express (Cisco Unified CME) to work with your network.

Note If you used Cisco Unified Communications Express - QCT to generate a basic telephony configuration, you can skip this module unless you want to modify the configuration to relay DHCP requests from IP phones to a DHCP server on a different router.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Network Parameters" section on page 135.

Contents

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 the "How to Configure VLANs on a Cisco Switch" section on page 73.

- 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. For installation information, see "Installing and Upgrading Cisco Unified CME Software" on page 87.
- 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 the *Enterprise QoS Solution Reference Network Design Guide.*

Information About Defining Network Parameters

To configure network parameters, you should understand the following concepts:

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 the "Defining a Single DHCP IP Address Pool" section on page 116.

- If your Cisco Unified CME router is the DHCP server and you need separate pools for non-IP-phone DHCP clients, see the "Defining a Separate DHCP IP Address Pool for Each DHCP Client" section on page 118.
- 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 the "Defining a DHCP Relay" section on page 120.

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 the "Enabling Network Time Protocol on the Cisco Unified CME Router" section on page 122.

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 the "Configuring DTMF Relay for H.323 Networks in Multisite Installations" section on page 123.

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 "Configuring SIP Trunk Support" section on page 124.

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. For configuration information, see the "Basic SIP Configuration" chapter in the *Cisco IOS SIP Configuration Guide*.

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 the "Configuring SIP Trunk Support" section on page 124.

Out-of-Dialog REFER

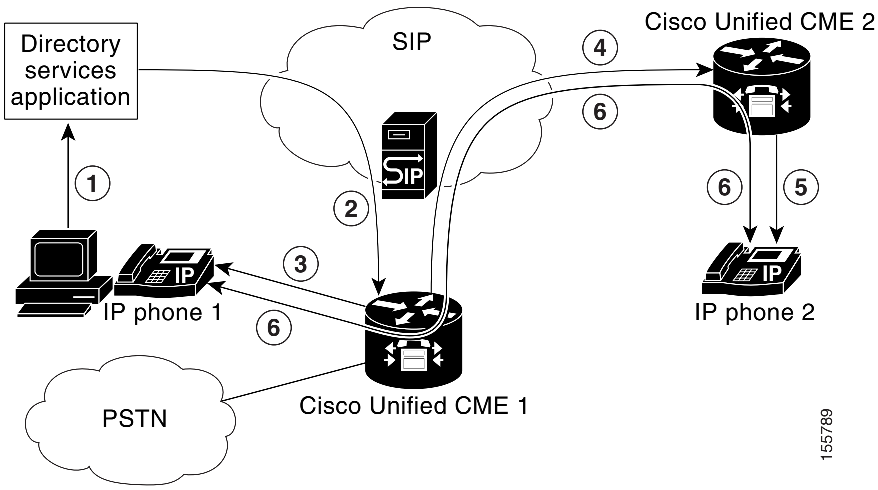
Out-of-dialog REFER (OOD-R) allows remote applications to establish calls by sending a REFER message to Cisco Unified CME without an initial INVITE. After the REFER is sent, the remainder of the call setup is independent of the application and the media stream does not flow through the application. The 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 6 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 6 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 the "Enabling OOD-R" section on page 128.

How to Define Network Parameters

This section contains the following tasks. You may not need to perform all of these procedures.

Enabling Calls in Your VoIP Network

To enable calls between endpoints in Cisco Unified CME, perform the following steps.

Restrictions

- 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.

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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	`enable` **Example:** `Router> 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 (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.

	Command or Action	Purpose
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. • Cisco Unified CME does not maintain a persistent database of registration entries across reloads. If the WAN is down and you reboot your Cisco Unified CME router, when the router reloads it will have no database of SIP phone registrations. The SIP phones will have to register again, which could take several minutes, as SIP phones do not use a keepalive functionality. We recommend that you change the expiry • **max** *sec*—(Optional) Range: 600 to 86400. Default: 3600. Recommended value: 600. • **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.
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.

	Command or Action	Purpose
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-voi-sip)# end`	Exits configuration mode and enters privileged EXEC mode.

Defining 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 Defining a Single DHCP IP Address Pool, page 116.
- 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 Defining a Separate DHCP IP Address Pool for Each DHCP Client, page 118.
- 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 Defining a DHCP Relay, page 120.

Defining a 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 the "Enabling Network Time Protocol on the Cisco Unified CME Router" section on page 122.

Prerequisites

Your Cisco Unified CME router is a DHCP server.

Restrictions

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

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.
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. See the "Enabling Network Time Protocol on the Cisco Unified CME Router" section on page 122.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see "Generating Configuration Files for Phones" on page 265.

Defining a 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 the "Enabling Network Time Protocol on the Cisco Unified CME Router" section on page 122.

Prerequisites

Your Cisco Unified CME router is a DHCP server.

Restrictions

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

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.
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.

	Command or Action	Purpose
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 the "Enabling Network Time Protocol on the Cisco Unified CME Router" section on page 122.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see "Generating Configuration Files for Phones" on page 265.

Defining a 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.

Prerequisites

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.

Restrictions

This Cisco Unified CME router cannot be the DHCP server.

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 the "Enabling Network Time Protocol on the Cisco Unified CME Router" section on page 122.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see "Generating Configuration Files for Phones" on page 265.

Enabling Network Time Protocol on the Cisco Unified CME Router

To enable NTP for the Cisco Unified CME router, perform this task.

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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	`enable` **Example:** `Router> 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.
Step 5	**ntp server** *ip-address* **Example:** `Router(config)# ntp server 10.1.2.3`	Synchronize 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 the "Configuring DTMF Relay for H.323 Networks in Multisite Installations" section on page 123.
- If Cisco Unified CME will interact with a SIP Gateway, you must set up support for the gateway. See the Configuring SIP Trunk Support, page 124.
- If you are configuring Cisco Unified CME for the first time on this router and you are ready to configure system parameters. See "Configuring System-Level Parameters" on page 137.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see "Generating Configuration Files for Phones" on page 265.

Configuring 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 the "Configuring SIP Trunk Support" on page 124.

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.

	Command or Action	Purpose
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 the Configuring SIP Trunk Support, page 124.
- If you are configuring Cisco Unified CME for the first time on this router and you are ready to configure system parameters. See "Configuring System-Level Parameters" on page 137.
- If you are finished modifying network parameters for an already configured Cisco Unified CME router, see "Generating Configuration Files for Phones" on page 265.

Configuring 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.
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.

	Command or Action	Purpose
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.

Verifying SIP Trunk Support Configuration

To verify SIP trunk configuration, perform the following steps:

SUMMARY STEPS

1. **show sip-ua status**
2. **show sip-ua timers**
3. **show sip-ua register status**
4. **show sip-ua statistics**

DETAILED STEPS

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.

```
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.

Changing the TFTP Address on a DHCP Server

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

Prerequisites

Your Cisco Unified CME router is a DHCP server.

Restrictions

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.

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.

	Command or Action	Purpose
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.

Enabling OOD-R

To enable OOD-R support on the Cisco Unified CME router, perform the following steps.

Prerequisites

- Cisco Unified CME 4.1 or a later version.
- Cisco IOS Release 12.4(11)XJ or a later release.
- 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)*.

Restrictions

- 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.

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.
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.

	Command or Action	Purpose
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.

Verifying OOD-R Configuration

Step 1 **show running-config**

This command verifies 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 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.

```
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 **debug ccsip messages**

This command displays the SIP messages exchanged between the SIP UA client and the router.

```
Router# debug ccsip messages

SIP Call messages tracing is enabled

Aug 22 18:15:35.757: //-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Received:
REFER sip:1011@10.5.2.141:5060 SIP/2.0
Via: SIP/2.0/UDP 172.18.204.144:59607;branch=z9hG4bK1238
From: <sip:1011@172.18.204.144>;tag=308fa4ba-4509
To: <sip:1001@10.5.2.141>
Call-ID: f93780-308fa4ba-0-767d@172.18.204.144
CSeq: 101 REFER
Max-Forwards: 70
Contact: <sip:1011@172.18.204.144:59607>
User-Agent: CSCO/7
Timestamp: 814720186
Refer-To: sip:1001@10.5.2.141
Referred-By: <sip:root@172.18.204.144>
Content-Length: 0


Aug 22 18:15:35.773: //-1/xxxxxxxxxxxx/SIP/Msg/ccsipDisplayMsg:
Sent:
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP 172.18.204.144:59607;branch=z9hG4bK1238
From: <sip:1011@172.18.204.144>;tag=308fa4ba-4509
To: <sip:1001@10.5.2.141>;tag=56D02AC-1E8E
Date: Tue, 22 Aug 2006 18:15:35 GMT
Call-ID: f93780-308fa4ba-0-767d@172.18.204.144
Timestamp: 814720186
CSeq: 101 REFER
Content-Length: 0
Contact: <sip:1011@172.18.204.141:5060>
```

Step 2 **debug voip application oodrefer**

This command displays debugging messages for the OOD-R feature.

```
Router# debug voip application oodrefer

voip application oodrefer debugging is on

Aug 22 18:16:21.625: //-1//AFW_:/C_ServiceThirdParty_Event_Handle:
Aug 22 18:16:21.625: //-1//AFW_:/AFW_ThirdPartyCC_New:
Aug 22 18:16:21.625: //-1//AFW_:EE461DC520000:/C_PackageThirdPartyCC_NewReq: ThirdPartyCC
module listened by TclModule_45F39E28_0_91076048
Aug 22 18:16:21.625: //-1//AFW_:EE461DC520000:/OCOpen_SetupRequest: Refer Dest1: 1011,
Refer Dest2: 1001; ReferBy User: root
Aug 22 18:16:21.693: //-1//AFW_:EE461DC520000:/OCHandle_SignalEvent_1:
Aug 22 18:16:21.693: //-1//AFW_:/Third_Party_CC_Send_Notify: Third_Party_CC_Send_Notify:
sending notify respStatus=2, final=FALSE, failureCause=16
Aug 22 18:16:21.693: //-1//AFW_:/Third_Party_CC_Send_Notify: AppNotify successful!
Aug 22 18:16:26.225: //-1//AFW_:EE461DC520000:/OCHandle_SignalEvent_1:
Aug 22 18:16:26.229: //-1//AFW_:EE461DC520000:/OCHandle_SignalEvent_1:
Aug 22 18:16:26.249: //-1//AFW_:EE461DC520000:/OCHandle_SignalEvent_2:
Aug 22 18:16:29.341: //-1//AFW_:EE461DC520000:/OCHandle_SignalEvent_2:
```

```
Aug 22 18:16:29.341: //-1//AFW_:/Third_Party_CC_Send_Notify: Third_Party_CC_Send_Notify:
sending notify respStatus=4, final=TRUE, failureCause=16
Aug 22 18:16:29.341: //-1//AFW_:/Third_Party_CC_Send_Notify: AppNotify successful!
Aug 22 18:16:29.349: //-1//AFW_:EE461DC520000:/OCHandle_Handoff: BAG contains:
Aug 22 18:16:29.349: LEG[895    ][LEG_INCCONNECTED(5)][Cause(0)]
Aug 22 18:16:29.349: CON[7      ][CONNECTION_CONFED(2)] {LEG[895
][LEG_INCCONNECTED(5)][Cause(0)],LEG[896    ][LEG_OUTCONNECTED(10)][Cause(0)]}
Aug 22 18:16:29.349: LEG[896    ][LEG_OUTCONNECTED(10)][Cause(0)]
Aug 22 18:16:29.365: //-1//AFW_:EE461DC520000:/OCAnyState_IgnoreEvent: Event Ignored
Aug 22 18:16:29.365: //-1//AFW_:/C_ServiceThirdParty_Event_Handle:
Aug 22 18:16:29.365: //-1//AFW_:EE461DC520000:/C_ServiceThirdParty_Event_Handle: Received
event APP_EV_NOTIFY_DONE[174] in Main Loop
Aug 22 18:16:29.365: //-1//AFW_:EE461DC520000:/OCAnyState_IgnoreEvent: Event Ignored
Aug 22 18:16:29.365: //-1//AFW_:/C_ServiceThirdParty_Event_Handle:
Aug 22 18:16:29.365: //-1//AFW_:EE461DC520000:/C_ServiceThirdParty_Event_Handle: Received
event APP_EV_NOTIFY_DONE[174] in Main Loop
Aug 22 18:16:29.369: //-1//AFW_:EE461DC520000:/OCHandle_SubscribeCleanup:
Aug 22 18:16:29.369: //-1//AFW_:EE461DC520000:/Third_Party_CC_Cleaner:
Aug 22 18:16:29.453: //-1//AFW_:EE461DC520000:/OCClosing_AnyEvent:
Aug 22 18:16:29.453: //-1//AFW_:EE461DC520000:/Third_Party_CC_Cleaner:
Aug 22 18:16:29.453: //-1//AFW_:EE461DC520000:/OCClosing_AnyEvent:
Aug 22 18:16:29.453: //-1//AFW_:EE461DC520000:/Third_Party_CC_Cleaner:
```

Configuration Examples for Network Parameters

- NTP Server: Example, page 132
- DTMF Relay for H.323 Networks: Example, page 132
- OOD-R: Example, page 133

NTP Server: Example

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: Example

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
```

OOD-R: Example

```
!
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 jack password 021201481F
 refer-ood enable
!
```

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 "Configuring System-Level Parameters" on page 137.
- 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 "Generating Configuration Files for Phones" on page 265

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Network Parameters

Table 9 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 9 lists the 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.

Table 9 Feature Information for Network Parameters

Feature Name	Cisco Unified CME Version	Modification
Out-of-Dialog Refer	4.1	Out-of Dialog REFER support was added.

Configuring System-Level Parameters

Last Updated: September 25, 2007

This chapter describes the system-level settings to configure before you add devices and configure Cisco Unified Communications Manager Express (Cisco Unified CME) features.

Note If you used Cisco Unified Communications Express - QCT to generate a basic telephony configuration, you can skip this module.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for System-Level Parameters" section on page 163.

Contents

Prerequisites for System-Level Parameters

- To support Cisco Unified IP phones that are running SIP to be connected directly to the Cisco Unified CME router, Cisco CME 3.4 or a later version must be installed on the router. For installation information, see "Installing and Upgrading Cisco Unified CME Software" on page 87.
- Cisco Unified CME must be configured to work with your IP network. For configuration information, see "Defining Network Parameters" on page 109.

Information About Configuring System-Level Parameters

To configure system-level parameters, you should understand the following concepts:

- Network Time Protocol for SIP Phones, page 138
- Per-Phone Configuration Files, page 138
- Redundant Cisco Unified CME Router, page 139
- Timeouts, page 140

Network Time Protocol for SIP Phones

SIP phones registered to a Cisco Unified CME router can synchronize to an NTP server. SIP phones can synchronize to the Cisco Unified CME router, however some routers can lose their clock after a reboot causing phones to display the wrong time. Synchronizing to an NTP server ensures that SIP phones maintain the correct time. You enable NTP for all SIP phones by using the **ntp-server** command in voice register global configuration mode. For configuration information, see the "SIP: Setting Network Time Protocol" section on page 157.

Per-Phone Configuration Files

In Cisco Unified CME 4.0 and later versions, you can use an external TFTP server to offload the TFTP server function on the Cisco Unified CME router. You can also use flash memory or slot 0 on the Cisco Unified CME router for this purpose. This additional storage capacity allows you to use different configuration files for each phone type or for each phone, which allows you to specify different user locales and network locales for different phones. Before this version, 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 the system is the storage location, there can be only one default configuration file and it is used for all phones in the system. All phones, therefore, use the same user locale and network locale. User-defined locales are not supported. To use the system location, either do not use the **cnf-file location** command to specify a location or use the **no cnf-file location** {**flash:** | **slot0:** | **tftp** *url*} command to reset the option from a previous, different location.
- Flash or slot 0—When flash 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. To store configuration files in flash or slot 0, use the **cnf-file location flash:** or **cnf-file location slot0:** command.

Note When the storage location chosen is flash and the file system type on this device is Class B (LEFS), check 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 using 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. To store configuration files on an external TFTP server, use the **cnf-file location tftp** *url* command.

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. To use the per-system option, either do not use the **cnf-file** command or use the **no cnf-file** command to reset the option from a different configuration.
- 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. To create configuration files per phone type, use the **cnf-file perphonetype** command. This option is not supported if you store the configuration files in the system 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 generates with the default user and network locale unless a different user and network locale is applied to the phone using an ephone template. To create configuration files per phone type, use the **cnf-file perphone** command. This option is not supported if you store the configuration files in the system location.

For configuration information, see the "SCCP: Defining Per-Phone Configuration Files and Alternate Location" section on page 147.

Redundant Cisco Unified CME Router

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 takes over and provides services seamlessly 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 with the **keepalive** command.

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 is operating normally, 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 reregisters with it. The reregistration 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 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 using the voice-port **ring number 3** command. 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 **ip source-address** command is used on both routers to specify the IP addresses of the primary and secondary routers.

Timeouts

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

- Busy Timeout—Amount of time that can elapse after a transferred call reaches a busy signal before the call is disconnected.
- Interdigit Timeout—Amount 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). For more information, see *Dial Peer Configuration on Voice Gateway Routers*.
- Ringing Timeout—Amount 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.

How to Configure System-Level Parameters

- Configuring Bulk Registration, page 141 (optional)

SCCP

- SCCP: Setting Up Cisco Unified CME, page 143 (required)
- SCCP: Setting Date and Time Parameters, page 145 (required)
- SCCP: Blocking Automatic Registration, page 146 (optional)
- SCCP: Defining Per-Phone Configuration Files and Alternate Location, page 147 (optional)
- SCCP: Changing Defaults for Time Outs, page 148 (optional)
- SCCP: Configuring a Redundant Router, page 150 (optional)

SIP

- SIP: Setting Up Cisco Unified CME, page 153 (required)
- SIP: Setting Date and Time Parameters, page 155 (required)
- SIP: Setting Network Time Protocol, page 157 (required)
- SIP: Changing Session-Level Application for SIP Phones, page 158 (optional)

Configuring 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, follow the steps in this section.

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

Note To specify that an individual directory number not register with the external registrar by using this command. For configuration information, see the "SIP: Disabling SIP Proxy Registration for a Directory Number" section on page 192.

Prerequisites

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.
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 SIP proxy server. • *number*—Unique sequence of up to 32 characters including wild cards and patterns that represents E.164 n umbers that will register with 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 Session Initiation Protocol (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 SIP proxy server.
Step 9	**end** **Example:** `Router(config-sip-ua)# end`	Exits 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
```

SCCP: Setting Up Cisco Unified CME

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tftp-server flash:***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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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	**tftp-server flash:***filename* **Example:** `Router(config)# tftp-server flash:P00307020300.bin`	Permits IP phones served by the Cisco Unified CME router to access the specified file in flash memory. • A separate **tftp-server flash** command is required for each phone type.
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`	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 phone type. **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, then load the larger file.
Step 6	**max-ephones** *max-phones* **Example:** `Router(config-telephony)# max-ephones 24`	Limits number of phones to be supported by this router. • Maximum number is platform and version-specific. Type **?** for value.
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.
Step 9	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Setting Date and Time Parameters

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **date-format** {**mm-dd-yy** | **dd-mm-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** {**mm-dd-yy** | **dd-mm-yy** | **yy-dd-mm** | **yy-mm-dd**} **Example:** `Router(config-telephony)# date-format yy-dd-mm`	(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 or 24-hour clock for the time display format on phone display. • Default: **12**.

	Command or Action	Purpose
Step 6	**time-zone** *number* **Example:** `Router(config-telephony)# time-zone 2`	Sets time zone used for all SCCP phones. • Required for Cisco Unified IP Phone 7970G and 7971G-GE. • Default: 5, Pacific Standard/Daylight Time (-480).
Step 7	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Blocking Automatic Registration

To prevent Cisco Unified IP phones that are not explicitly configured in Cisco Unified CME from registering with the Cisco Unified CME router, perform the following steps.

Prerequisite

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

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

	Command or Action	Purpose
Step 4	**auto-reg-ephone** **Example:** `Router(config-telephony)# no auto-reg-ephone`	Enables all Cisco Unified IP phones that are running SCCP to register regardless of whether the phone is explicitly configured in Cisco Unified CME. • Default: Enabled
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Defining Per-Phone Configuration Files and Alternate Location

To define a location other than system for storing configuration files and to specify what type of configuration files to generate, perform the following steps. To use multiple network and user locales, or user-defined locales, you must define per-phone or per-phone type configuration files

Prerequisites

Cisco Unified CME 4.0 or a later version.

Restrictions

- 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.
- For 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. **cnf-file location** {**flash:** | **slot0:** | **tftp** *tftp-url*}
5. **cnf-file** {**perphonetype** | **perphone**}
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	**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.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

What to Do Next

If you changed the configuration file storage location, use the **option 150 ip** command to update the address. See "Changing the TFTP Address on a DHCP Server" on page 127.

SCCP: Changing Defaults for Time Outs

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 amount 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. • The default is usually adequate. If the interval is set too large, it is possible that notification will 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.

SCCP: Configuring a Redundant Router

To configure a secondary Cisco Unified CME router to act as a backup if the primary router fails, perform the following steps on both the primary and secondary Cisco Unified CME routers.

Prerequisites

- Cisco Unified CME 4.0 or a later version.
- The secondary router must have a running configuration identical to that of the primary router.
- The physical configuration of the secondary router must be as described in the "Redundant Cisco Unified CME Router" section on page 139.
- 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.

	Command or Action	Purpose
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 secondary 10.2.2.25`	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 SCCP. Range is 2000 to 9999. Default is 2000. • **secondary** *ip-address*—Indicates a backup Cisco Unified CME router. • **rehome** *seconds*—Not used by Cisco 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.
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.

	Command or Action	Purpose
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 secondary 10.2.2.25`	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 SCCP. Range is 2000 to 9999. Default is 2000. • **secondary** *ip-address*—Indicates a backup Cisco Unified CME router. • **rehome** *seconds*—Not used by Cisco 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.
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.

	Command or Action	Purpose
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.

SIP: Setting Up Cisco Unified CME

To identify filenames and 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.

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.

Prerequisites

- Cisco CME 3.4 or a later version.

Restrictions

- 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 Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE, are supported only in Cisco Unified CME 4.1 and later.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **mode cme**
5. **source-address** *ip-address*
6. **load** *phone-type firmware-file*
7. **tftp path** {**system:** | **flash:** | **slot0:** | **tftp** *tftp-url*}
8. **max-pool** *max-phones*

9. **max-dn** *max-directory-numbers*
10. **authenticate** [**all**] [**realm** *string*]
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 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**—(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** {**system:** | **flash:** | **slot0:** | **tftp:** *tftp-url*} **Example:** `Router(config-register-global)# tftp-path http://mycompany.com/files`	Defines the location from which the SIP phones will download configuration profile files. • Default: **system**.
Step 8	**max-pool** *max-phones* **Example:** `Router(config-register-global)# max-pool 10`	Limits number of SIP phones to be supported by the Cisco Unified CME router. • Default: 0.

	Command or Action	Purpose
Step 9	**max-dn** *max-directory-numbers* **Example:** `Router(config-register-global)# max-dn 20`	(Optional) Limits number of directory numbers for SIP phones to be supported by the Cisco Unified CME router. • Default: 150 or maximum allowed on platform, by version. 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	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

SIP: Setting Date and Time Parameters

To specify the format of the date and time that appears on all SIP phones in Cisco Unified CME, follow the steps in this section.

Prerequisites

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **timezone** *number*
5. **date-format** [**d/m/d** | **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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> 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-m-d* | 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**.
Step 7	**dst auto-adjust** **Example:** `Router(config-register-global)# dst auto-adjust`	(Optional) Enables automatic adjustment of daylight savings 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 savings time on SIP phones in Cisco Unified CME. • Required if automatic adjustment of daylight savings time is enabled by using the **dst auto-adjust** command. • Default is Start: First week of April, Sunday, 2:00 a.m and Stop: Last week of October, Sunday 2:00 a.m.
Step 9	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

SIP: Setting Network Time Protocol

To enable NTP for Java-based phones, such as the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE, connected to Cisco Unified CME running SIP, perform this task.

Prerequisites

- 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 the "SIP: Upgrading or Downgrading Phone Firmware Between Versions" section on page 95.

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`	Clock on this router is synchronized with the specified NTP server.
Step 5	`end` **Example:** `Router(config-register-global)# end`	Returns to privileged EXEC mode.

SIP: Changing Session-Level Application for SIP Phones

To change a the default session-level application for all SIP phones, perform the following steps.

Prerequisites

- 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.
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** The **application** command in voice register pool configuration mode takes precedence over this command in voice register global configuration mode.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuration Examples for System-Level Parameters

This section contains the following examples:

System-Level Parameters: Example

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 Phone 7905, 7912, 7914, 7920, 7940, and 7960 phone types and 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
.
.
.
```

Blocking Automatic Registration: Example

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
```

Redundant Router: Example

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 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
```

Where to Go Next

After configuring system-level parameters, you are ready to configure phones in Cisco Unified CME for making basic calls. See "Configuring Phones to Make Basic Calls" on page 165.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for System-Level Parameters

Table 10 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 10 lists the 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.

Table 10 Feature Information for System-Level Parameters

Feature Name	Cisco Unified CME Versions	Feature Information
Blocking Automatic Registration	4.0	IP phones that are not explicitly configured in Cisco Unified CME are blocked from registering.
Bulk Registration	3.4	Bulk registration for registering a block of phone numbers with an external registrar was introduced.
Network Time Protocol for SIP Phones	4.1	SIP phones can synchronize to an NTP server.
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	4.0	Redundant router capability was introduced.
SIP phones in Cisco Unified CME	3.4	Support for SIP endpoints directly connected to Cisco Unified CME was introduced.

Configuring Phones to Make Basic Calls

Last Updated: September 25, 2007

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

Note If you used Cisco Unified Communications Express - QCT to generate a basic telephony configuration, you can skip this module unless you want to modify the configuration to add phones.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Configuring Phones to Make Basic Calls" section on page 230.

Contents

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 "Installing and Upgrading Cisco Unified CME Software" on page 87.
- For Cisco Unified IP phones that are running SIP and are connected directly to Cisco Unified CME, Cisco Unified CME 3.4 or later must be installed on the router. See "Installing and Upgrading Cisco Unified CME Software" on page 87.
- Procedures in "Defining Network Parameters" on page 109 and "Configuring System-Level Parameters" on page 137 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

To configure phones to make basic calls, you should understand the following concepts:

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.

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.

The number of directory numbers that you create corresponds to the number of simultaneous calls that you can have, because each directory number represents a virtual voice port in the router. 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 number 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 number in a Cisco Unified CME system:

- Single-Line, page 168
- Dual-Line, page 168
- Two Directory Numbers with One Telephone or Extension Number, page 169
- Dual-Number, page 170
- Shared, page 170
- Monitor Mode for Shared Lines, page 172
- Overlaid, page 171

Single-Line

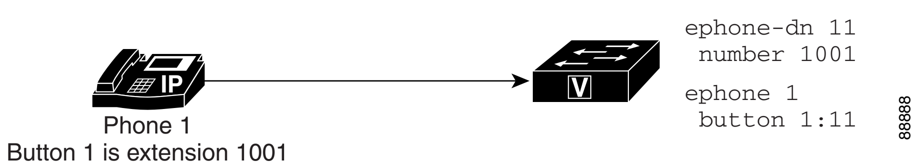
A single-line directory number has the following characteristics:

- 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.
- When used with multiple-line features like call waiting, call transfer, and conferencing, there must be more than one single-line directory number on a phone.
- Can be combined with dual-line directory numbers on the same phone.

Note that 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 shows a single-line directory number for an SCCP phone in Cisco Unified CME.

Figure 7 Single-Line Directory Number



Dual-Line

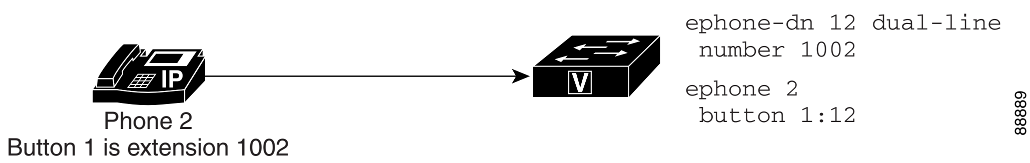
A dual-line directory number has the following characteristics:

- 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 that 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 8 shows a dual-line directory number for an SCCP phone in Cisco Unified CME.

Figure 8 Dual-Line Directory Number



Two Directory Numbers with One Telephone or Extension Number

Two directory numbers with one 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 on page 170 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 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, 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 the “Shared” section on page 170.

The examples in Figure 9 and Figure 10 show how two directory numbers with one number are used to provide a small hunt group capability. In Figure 9, 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

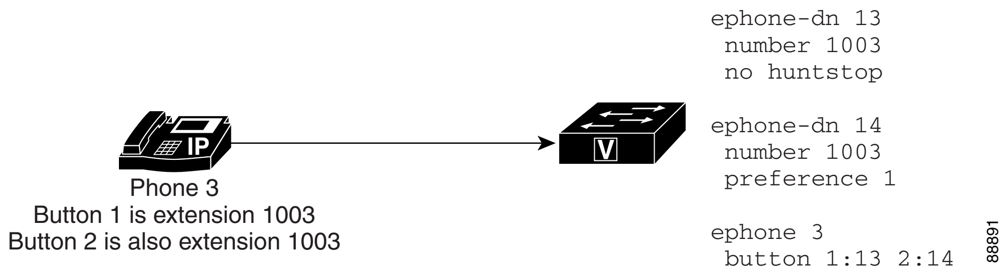
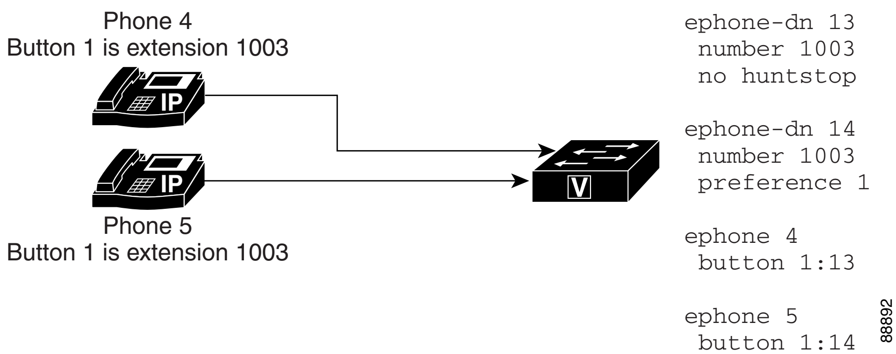


Figure 10 Two Directory Numbers with One Number on Two Phones



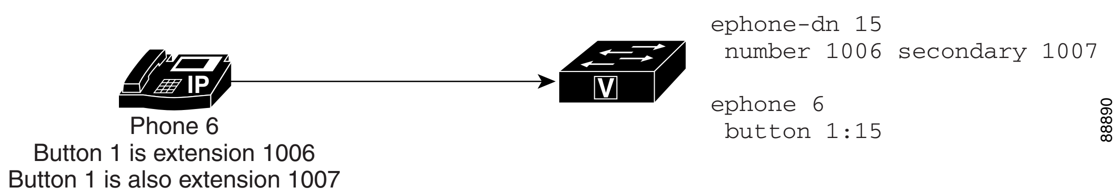
Dual-Number

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 shows a directory number that has two numbers, extension 1006 and extension 1007.

Figure 11 Dual-Number Directory



Shared

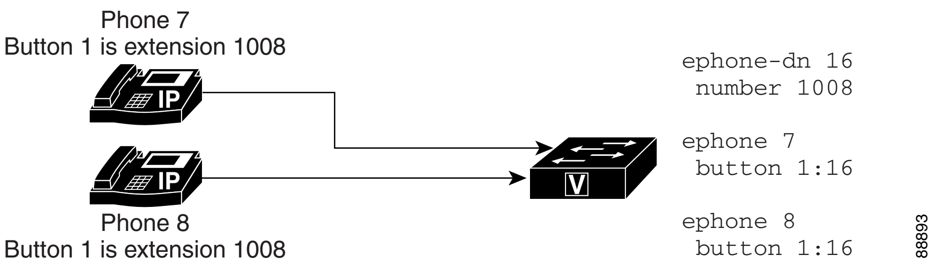
A shared directory number has the following characteristics:

- Line 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 these phones share the same directory number, if the directory number is connected to a call on one phone, that directory number is unavailable for other calls on the second 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.

Figure 12 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



Overlaid

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 "Configuring Call-Coverage Features" on page 581.

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 ten lines in an overlay set shared by ten phones, resulting in the possibility of ten simultaneous calls to the same number. For configuration information, see the "SCCP: Creating Directory Numbers for a Simple Key System" section on page 196

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.

When the line is in use, it cannot be used for incoming or outgoing calls. A monitor-line lamp can be 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 line button for a monitored line can also be used as a direct-station-select for a call transfer when the monitored line is in an idle state. In this case, 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 configuration information, see the "SCCP: Assigning Directory Numbers to Phones" section on page 179.

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 the "Watch Mode for Phones" section on page 172.

For BLF monitoring of speed-dial buttons and directory call-lists, see "Configuring Presence Service" on page 843.

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 Busy Lamp Field (BLF) notification for all lines on another phone (watched phone) for which the 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. The line and line button on the watching phone are available in watch mode for visual status only. Calls cannot be made or received using a line button that has been set in watch mode. 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 direct-station-select 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 the "SCCP: Assigning Directory Numbers to Phones" section on page 179.

Note 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 the "Monitor Mode for Shared Lines" section on page 172.

For BLF monitoring of speed-dial buttons and directory call-lists, see "Configuring Presence Service" on page 843.

PSTN FXO Trunk Lines

In Cisco CME 3.2 and later, IP phones running SCCP can be configured to have buttons for dedicated PSTN FXO trunk lines, also known as FXO lines. FXO lines may 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 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 nonPSTN 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 soft key.

In Cisco Unified CME 4.0, 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 the "SCCP: Configuring Trunk Lines for a Key System" section on page 199.

Analog Phones

Cisco Unified CME supports analog phones using Cisco Analog Telephone Adaptors (ATAs) or FXS ports in SCCP mode or H.323 mode, and supports fax machines on Cisco ATA or FXS ports in H.323 mode. The FXS ports used for analog phones or fax can be on the Cisco Unified CME router or on a Cisco VG 224 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. Each Cisco ATA enables two analog phones to function as IP phones. For configuration information, see the "Configuring Cisco ATA Support" section on page 209.

FXS Ports in SCCP Mode

FXS ports on Cisco VG 224 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 *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways*.

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 that 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.

The following links provide details on configuring analog phone features for FXS ports in H.323 mode:

- "Configuring Analog Voice Ports" section in *Voice Ports Configuration Guide*
- "Caller ID" section of the *Cisco IOS Voice Configuration Library* for your Cisco IOS release
- "Modem Support for VoIP" section of the *Cisco IOS Voice Configuration Library* for your Cisco IOS release
- *Cisco IOS Fax and Modem Services over IP Application Guide* for your Cisco IOS release

Remote Teleworker Phones

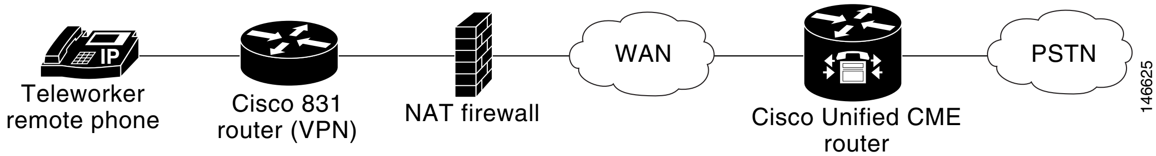
IP phones or instances of Cisco IP Communicator can be connected to a Cisco Unified CME system over a wide area network (WAN) to support teleworkers who have offices that are remote from the Cisco Unified CME router. The maximum number of remote phones that can be supported is determined by the available 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 nonroutable private IP addresses and the hub Cisco Unified CME router uses a globally routable address (see Figure 13). 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 (or example, a Cisco 831) and the Cisco Unified CME router. This solution requires an 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 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 the "SCCP: Enabling a Remote Phone" section on page 216.

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 affect on a call directed through a VoIP dial peer unless the **dspfarm-assist** keyword is also used.

For configuration information, see the "SCCP: Enabling a Remote Phone" section on page 216.

For information about transcoding behavior when using the G.729r8 codec, see the "Transcoding When a Remote Phone Uses G.729r8" section on page 325.

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 soft key or # key, or wait for the interdigit-timeout to trigger call processing. In Cisco United CME 4.1 and later, two methods of collecting and matching digits are supported for SIP phones, depending on the model of phone:

- KPML Digit Collection, page 176
- SIP Dial Plans, page 176

KPML 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 soft key 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 the "SIP: Enabling KPML" section on page 189.

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 soft key or # key, or to wait for the interdigit timeout to trigger an outgoing INVITE. You configure a SIP dial plan and associate the dial plan with a SIP phone. The dial plan is downloaded to the phone in the configuration file.

You can configure SIP dial plans and associate them with the following SIP phones:

- Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE—These phones use dial plans and support KPML. If both a dial plan and KPML are enabled, the dial plan has priority.

  If a matching dial plan is not found and KPML is disabled, the user must wait for the interdigit timeout before the SIP NOTIFY message is sent to Cisco Unified CME. Unlike other SIP phones, these phones do not have a Dial soft key to indicate the end of dialing, except when on-hook dialing is used. In this case, the user can press the Dial soft key at any time to send all the dialed digits to Cisco Unified CME.

- Cisco Unified IP Phone 7905, 7912, 7940, and 7960—These phones use dial plans and do not support KPML. If you do not configure a SIP dial plan for these phones, or if the dialed digits do not match a dial plan, the user must press the Dial soft key or wait for the interdigit timeout before digits are sent to Cisco Unified 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 Phone 7905 and 7912—The dial plan is a field in their configuration files.
- Cisco Unified IP Phone 7911G, 7940, 7941G, 7941GE, 7960, 7961G, 7961GE, 7970G, and 7971GE—The dial plan is a separate XML file that is pointed to from the normal configuration file.

For configuration information for Cisco Unified CME, see the "SIP: Configuring Dial Plans" section on page 184.

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 the "SIP: Selecting Session-Transport Protocol for a Phone" section on page 191.

How to Configure Phones for a PBX System

This section contains the following tasks:

SCCP: Creating Directory Numbers

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 "SCCP: Configuring Overlaid Ephone-dns" on page 633.

Prerequisites

- The maximum number of directory numbers must be configured for other than the default, by using the **max-dn** command.

Restrictions

- 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 the "How to Configure Phones for a Key System" section on page 196.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
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	**ephone-dn** *dn-tag* [**dual-line**] **Example:** `Router(config)# ephone-dn 55 dual-line`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status. • Configuring a dual-line supports features such as call waiting, call transfer, and conferencing with a single ephone-dn. • To change an ephone-dn from dual-line to single-line mode or the reverse, you must first delete the ephone-dn and then recreate it.

	Command or Action	Purpose
Step 4	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 2345`	Configures a valid extension number for this ephone-dn instance. • Configuring a secondary number supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.
Step 5	**name** *name* **Example:** `Router(config-ephone-dn)# name Smith, John`	(Optional) Associates a name with this directory number. 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-telephony)# end`	Returns to privileged EXEC mode.

What to Do Next

After creating directory numbers, you can assign one or more directory number to a Cisco Unified IP phone. See "SCCP: Assigning Directory Numbers to Phones" section on page 179.

SCCP: Assigning Directory Numbers to Phones

This task sets up the initial ephone-dn-to-ephone relationships—that is, 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.

Note To create and assign directory numbers to be included in an overlay set, see "SCCP: Configuring Overlaid Ephone-dns" on page 633.

Prerequisites

- 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.

Restrictions

- 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 "Configuring Automatic Line Selection" on page 479

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. **keypad-normalize**
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 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 Cisco Unified CME 3.0 and later, not required to register phones before configuring the phone because Cisco Unified CME 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`*`]]` **Example:** `Router(config-ephone)# type 7960 addon 1 7914`	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**.

	Command or Action	Purpose
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 Cisco Unified IP Phone 7910 has only one line button, but can be given two ephone-dn tags.
Step 7	**keypad-normalize** **Example:** `Router(config-ephone)# keypad-normalize`	(Optional) Imposes a 200-millisecond delay before each keypad message from an IP phone.
Step 8	**end** **Example:** `Router(config-telephony)# 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 the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- 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 "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

Examples

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
```

SIP: Creating Directory Numbers

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. Each directory number becomes a virtual line, or extension, on which call connections can be made. Each directory number configuration automatically creates one or more virtual dial peers and virtual voice ports to make those call connections.

Prerequisites

- Cisco CME 3.4 or a later version.

- The maximum number of directory numbers supported by a router is version and platform dependent. To configure more directory numbers than the default, use the **max-dn (voice register global)** command before performing this procedure. For configuration information, see "SIP: Setting Up Cisco Unified CME" on page 153.

Restrictions

- Call forward all, presence, and message-waiting indication (MWI) features in Cisco Unified CME 4.1 and later versions require that SIP phones are configured with a directory number (using **dn** keyword in **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.
- Shared lines are not supported by SIP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **number** *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 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	`end` **Example:** `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

SIP: Assigning Directory Numbers to 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 also 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 mac** *address*
5. **type** *phone-type*
6. **number** *tag* **dn** *dn-tag*
7. **username** *name* **password** *string*
8. **dtmf-relay** [**cisco-rtp**] [**rtp-nte**] [**sip-notify**]
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 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	**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.

	Command or Action	Purpose
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	**username** user*name* **password** *string* **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 8	**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 being configured to relay DTMF tones. **Note** SIP phones natively support in-band DTMF relay as specified in RFC 2833.
Step 9	**end** **Example:** `Router(config-register-pool)# end`	Exits 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 the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- If you want to select the session-transport protocol for a SIP phone, see the "SIP: Selecting Session-Transport Protocol for a Phone" section on page 191.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

SIP: Configuring Dial Plans

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 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.

Prerequisites

- Cisco Unified CME 4.1 or a later version.
- **mode cme** command must be enabled in Cisco Unified CME.

Restrictions

- 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.......
 pattern 3 .
```

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.

	Command or Action	Purpose
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. • 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 with the **max-pool** command.

	Command or Action	Purpose
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
```

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 "Generating Configuration Files for Phones" on page 265.

SIP: Verifying Dial Plan Configuration

Step 1 **show voice register dialplan** *tag*

This command displays the configuration information for a specific SIP dial plan.

```
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.

```
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.

```
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
```

SIP: Enabling KPML

To enable KPML digit collection on a SIP phone, perform the following steps.

Prerequisites

- Cisco Unified CME 4.1 or a later version.

Restrictions

- This feature is supported only on Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.
- A dial plan assigned to a phone has priority over KPML.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **voice register pool** *pool-tag*
4. **digit collect kpml**
5. **end**
6. **show voice register dial-peer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> 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 with 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 "Generating Configuration Files for Phones" on page 265.

SIP: Selecting Session-Transport Protocol for a Phone

To change the session-transport protocol for a SIP phone to TCP, from the default of UDP, perform the following steps.

Prerequisites

- Cisco Unified CME 4.1 or a later version.
- SIP phone to which configuration is to be applied must be already configured. For configuration information, see the "SIP: Assigning Directory Numbers to Phones" section on page 183.

Restrictions

- 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 using this command, calls to that phone will not complete successfully. The phone can originate calls, but it uses UDP, although TCP has been assigned.

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 configuration mode and enters privileged EXEC mode.

What to Do Next

- If you want to disable SIP Proxy registration for an individual directory number, see the "SIP: Disabling SIP Proxy Registration for a Directory Number" section on page 192.
- If you have SIP and SCCP phones connected to the same Cisco Unified CME, see the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See "SIP: Generating Configuration Profiles for SIP Phones" on page 270

SIP: Disabling 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.

Prerequisites

- Cisco Unified CME 3.4 or a later version.
- Bulk registration is configured at system level. For configuration information, see "Configuring Bulk Registration" on page 141.

Restrictions

- Phone numbers that are registered under voice register dn must belong to a SIP phone that is itself registered in Cisco Unified CME.

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`	Causes directory number being configured to not register with an external proxy server.
Step 6	`end` **Example:** `Router(config-register-dn)# end`	Exits 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 the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See "SIP: Generating Configuration Profiles for SIP Phones" on page 270

Configuring Codec for Local Calling Between SIP and SCCP Phones

To designate a codec for individual phones to ensure connectivity between SIP and SCCP phones connected to the same Cisco Unified CME router, perform the following steps for each SIP *or* SCCP phone.

Note If codec values for the dial peers of an internal connection do not match, the call fails.

Prerequisites

- Cisco Unified CME 3.4 or a later version.
- Cisco Unified IP phone to which codec is to be applied must be already configured. For configuration information for SIP phones, see the "SIP: Assigning Directory Numbers to Phones" section on page 183. For configuration information for SCCP phones, see the "SCCP: Assigning Directory Numbers to Phones" section on page 179.

Restrictions

- Required only if you have SIP and SCCP phones connected to the same Cisco Unified CME router.
- Modify the configuration for either SIP or SCCP phones to ensure that the codec for all phones match. Do not modify the configuration for SIP *and* SCCP phones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *ephone-tag*
   or
   voice register *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.

	Command or Action	Purpose
Step 3	**ephone** *ephone-tag* or **voice register pool** *pool-tag* **Example:** `Router(config)# ephone 3` or `Router(config)# voice register pool 3`	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 dynamically created when the SIP phone being configured, registers. • This command overrides any previously configured codec selection set with the **voice-class codec** command. • 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 2nd port of the Cisco ATA device, it will be disconnected gracefully. If a you want to use both Cisco ATA ports simultaneously, then configure G.711 in Cisco Unified CME. • 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 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 the "SIP: Selecting Session-Transport Protocol for a Phone" section on page 191.
- If you are finished configuring SIP phones to make basic calls using, you are ready to generate configuration files for the phones to be connected. See "SIP: Generating Configuration Profiles for SIP Phones" on page 270.
- 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 "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

How to Configure Phones for a Key System

This section contains the following tasks:

- SCCP: Creating Directory Numbers for a Simple Key System, page 196 (required)
- SCCP: Configuring Trunk Lines for a Key System, page 199 (required)
- SCCP: Configuring Individual IP Phones for Key System, page 207 (required)

SCCP: Creating Directory Numbers for a Simple Key System

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.

Restrictions

- 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` **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 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. • Increment 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** **Example:** `Router(config-ephone-dn)# no huntstop` or **huntstop** **Example:** `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.

Examples

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
```

SCCP: Configuring Trunk Lines for a Key System

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 the "SCCP: Configuring a Simple Key System Phone Trunk Line Configuration" section on page 199
- To enable direct status monitoring and allow transferred PSTN FXO line calls to be automatically recalled if the transfer target does not answer, see the "SCCP: Configuring an Advanced Key System Phone Trunk Line Configuration" section on page 202.

SCCP: Configuring a Simple Key System Phone Trunk Line Configuration

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.

Prerequisites

- 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
```

Restrictions

- A 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 soft keys.
- 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 VG 224 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.
- Transfer-to button optimization is not supported for call forwarding, call-park recall, call pickup on hold, or call pickup at alert.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **trunk** *digit-string* [**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.

	Command or Action	Purpose
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 a foreign exchange office (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 VG 224 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 the "SCCP: Configuring Individual IP Phones for Key System" section on page 207.

SCCP: Configuring an Advanced Key System Phone Trunk Line Configuration

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.

Prerequisites

- 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
```

Restrictions

- An 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 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 soft keys.
- 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 VG 224 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 VG 224 or Cisco ATA 180 Series.

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 purposes 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 in order 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.

	Command or Action	Purpose
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 a foreign exchange office (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. • The **monitor-port** and **transfer-timeout** keywords are not supported on directory numbers for analog ports on the Cisco VG 224 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 in order 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
```

SCCP: Configuring Individual IP Phones for Key System

To assign button numbers, line characteristics, and directory numbers to buttons on an individual phone to operate as a key system phone, perform the following steps.

Restrictions

- 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 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 the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see "SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G" on page 943.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

How to Configure Cisco ATA, Analog Phone Support, Remote Phones, and Cisco IP Communicator

This section contains the following tasks:

- SCCP: Configuring Cisco IP Communicator Support, page 218 (required)
- SCCP: Troubleshooting Cisco IP Communicator Support, page 219 (optional)

Configuring Cisco ATA Support

To enable an analog phone that uses a Cisco ATA to register with Cisco Unified CME, perform the following steps.

Restrictions

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 the *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0)*.

SUMMARY STEPS

1. Install Cisco ATA.
2. Configure Cisco ATA for SCCP.
3. Upgrade firmware.
4. Set network parameters on Cisco ATA.
5. Configure analog phones in Cisco Unified CME.

DETAILED STEPS

Step 1 Install the Cisco ATA. See the "Installing the Cisco ATA" chapter in the 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 the *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0).*

Step 3 Upgrade 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 "Installing and Upgrading Cisco Unified CME Software" on page 87. Alternatively, you can use a manual method, as described in the "Upgrading the Cisco ATA Signaling Image" chapter of the *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP (version 3.0)*.

Step 4 Configure the Cisco ATA to set the following parameters:

- 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 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 the "SCCP: Creating Directory Numbers" section on page 177.

What to Do Next

- If you have SIP *and* SCCP phones connected to the same Cisco Unified CME, see the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see "SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G" on page 943.
- If you are finished configuring phones to make basic calls, you are ready to generate configuration files for the phones to be connected. See "SCCP: Generating Configuration Files for SCCP Phones" on page 267 and "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

Verifying 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. For more information, see the *Cisco IOS Debug Command Reference* for your Cisco IOS release.

The following is sample output for two analog phones using a Cisco ATA with MAC address 000F.F758.E70E. The sample shows the activities that take place when the phones register.

```
Router# debug ephone detail mac-address 000F.F758.E70E

*Apr  5 02:50:11.966: New Skinny socket accepted [1] (33 active)
*Apr  5 02:50:11.970: sin_family 2, sin_port 15325, in_addr 1.4.188.72
*Apr  5 02:50:11.970: skinny_add_socket 1 1.4.188.72 15325
21:21:49: %IPPHONE-6-REG_ALARM: Name=ATA000FF758E70E Load=ATA030203SCCP051201A.zup
Last=Initialized
*Apr  5 02:50:11.974:
Skinny StationAlarmMessage on socket [2] 1.4.188.72 ATA000FF758E70E
*Apr  5 02:50:11.974: severityInformational p1=0 [0x0] p2=0 [0x0]
*Apr  5 02:50:11.974: Name=ATA000FF758E70E Load=ATA030203SCCP051201A.zup Last=Initialized
*Apr  5 02:50:12.066: ephone-(30)[2] StationRegisterMessage (29/31/48) from 1.4.188.72
*Apr  5 02:50:12.066: ephone-(30)[2] Register StationIdentifier DeviceName ATA000FF758E70E
*Apr  5 02:50:12.070: ephone-(30)[2] StationIdentifier Instance 1    deviceType 12
*Apr  5 02:50:12.070: ephone-30[-1]:stationIpAddr 1.4.188.72
*Apr  5 02:50:12.070: ephone-30[-1]:maxStreams 0
*Apr  5 02:50:12.070: ephone-30[-1]:protocol Ver 0x1
*Apr  5 02:50:12.070: ephone-30[-1]:phone-size 5392 dn-size 632
*Apr  5 02:50:12.070: ephone-(30) Allow any Skinny Server IP address 1.4.188.65
*Apr  5 02:50:12.070: ephone-30[-1]:Found entry 29 for 000FF758E70E
*Apr  5 02:50:12.070: ephone-30[-1]:socket change -1 to 2
*Apr  5 02:50:12.070: ephone-30[-1]:FAILED: CLOSED old socket -1
*Apr  5 02:50:12.074: ephone-30[2]:phone ATA000FF758E70E re-associate OK on socket [2]
21:21:49: %IPPHONE-6-REGISTER: ephone-30:ATA000FF758E70E IP:1.4.188.72 Socket:2
DeviceType:Phone has registered.
*Apr  5 02:50:12.074: Phone 29 socket 2
*Apr  5 02:50:12.074: Phone 29 socket 2: Running Bravo ??
*Apr  5 02:50:12.074: Skinny Local IP address = 1.4.188.65 on port 2000

*Apr  5 02:50:12.074: Skinny Phone IP address = 1.4.188.72 15325
*Apr  5 02:50:12.074: ephone-30[2]:Signal protocol ver 8 to phone with ver 1
*Apr  5 02:50:12.074: ephone-30[2]:Date Format M/D/Y
*Apr  5 02:50:12.078: ephone-30[2]:RegisterAck sent to ephone 2: keepalive period 30 use
sccp-version 1
*Apr  5 02:50:12.078: ephone-30[2]:CapabilitiesReq sent
*Apr  5 02:50:12.090: ephone-30[2]:VersionReq received
*Apr  5 02:50:12.090: ephone-30[2]:Version String not needed for ATA device. Part of XML
file
*Apr  5 02:50:12.090: ephone-30[2]:Version Message sent
*Apr  5 02:50:12.094: ephone-30[2]:CapabilitiesRes received
*Apr  5 02:50:12.098: ephone-30[2]:Caps list 7
G711Ulaw64k  60 ms
G711Alaw64k  60 ms
G729  60 ms
G729AnnexA  60 ms
G729AnnexB  60 ms
G729AnnexAwAnnexB  60 ms
Unrecognized Media Type 257  60 ms

*Apr  5 02:50:12.098: ephone-30[2]:ButtonTemplateReqMessage
*Apr  5 02:50:12.098: ephone-30[2]:StationButtonTemplateReqMessage set max presentation
to 2
*Apr  5 02:50:12.098: ephone-30[2]:CheckAutoReg
*Apr  5 02:50:12.102: ephone-30[2]:AutoReg is disabled
*Apr  5 02:50:12.102: ephone-30[2][ATA000FF758E70E]:Setting 1 lines 4 speed-dials on phone
(max_line 2)
*Apr  5 02:50:12.102: ephone-30[2]:First Speed Dial Button location is 2 (0)
*Apr  5 02:50:12.102: ephone-30[2]:Configured 4 speed dial buttons
*Apr  5 02:50:12.102: ephone-30[2]:ButtonTemplate lines=1 speed=4 buttons=5 offset=0
*Apr  5 02:50:12.102: ephone-30[2]:Skinny IP port 16384 set for socket [2]
*Apr  5 02:50:12.126: ephone-30[2]:StationSoftKeyTemplateReqMessage
*Apr  5 02:50:12.126: ephone-30[2]:StationSoftKeyTemplateResMessage
*Apr  5 02:50:12.206: ephone-30[2]:StationSoftKeySetReqMessage
*Apr  5 02:50:12.206: ephone-30[2]:StationSoftKeySetResMessage
```

```
*Apr  5 02:50:12.307: ephone-30[2]:StationLineStatReqMessage from ephone line 1
*Apr  5 02:50:12.307: ephone-30[2]:StationLineStatReqMessage ephone line 1 DN 80 = 8080
desc = 8080 label =
*Apr  5 02:50:12.307: ephone-30[2][ATA000FF758E70E]:StationLineStatResMessage sent to
ephone (1 of 2)
*Apr  5 02:50:12.427: ephone-30[2]:StationSpeedDialStatReqMessage speed 9
*Apr  5 02:50:12.427: ephone-30[2]:No speed-dial set 9
*Apr  5 02:50:12.427: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:12.547: ephone-30[2]:StationSpeedDialStatReqMessage speed 8
*Apr  5 02:50:12.547: ephone-30[2]:No speed-dial set 8
*Apr  5 02:50:12.547: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:12.635: ephone-30[2]:StationSpeedDialStatReqMessage speed 7
*Apr  5 02:50:12.635: ephone-30[2]:No speed-dial set 7
*Apr  5 02:50:12.635: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:12.707: New Skinny socket accepted [1] (34 active)
*Apr  5 02:50:12.707: sin_family 2, sin_port 15400, in_addr 1.4.188.72
*Apr  5 02:50:12.711: skinny_add_socket 1 1.4.188.72 15400
*Apr  5 02:50:12.711: ephone-30[2]:StationSpeedDialStatReqMessage speed 6
*Apr  5 02:50:12.711: ephone-30[2]:No speed-dial set 6
*Apr  5 02:50:12.715: ephone-30[2]:StationSpeedDialStatMessage sent
21:21:50: %IPPHONE-6-REG_ALARM: Name=ATA0FF758E70E01 Load=ATA030203SCCP051201A.zup
Last=Initialized
*Apr  5 02:50:12.715:
Skinny StationAlarmMessage on socket [3] 1.4.188.72 ATA000FF758E70E
*Apr  5 02:50:12.715: severityInformational p1=0 [0x0] p2=0 [0x0]
*Apr  5 02:50:12.715: Name=ATA0FF758E70E01 Load=ATA030203SCCP051201A.zup Last=Initialized
*Apr  5 02:50:12.811: ephone-30[2]:StationSpeedDialStatReqMessage speed 5
*Apr  5 02:50:12.811: ephone-30[2]:No speed-dial set 5
*Apr  5 02:50:12.811: ephone-30[2]:StationSpeedDialStatMessage sent
21:21:50: %IPPHONE-6-REGISTER: ephone-31:ATA0FF758E70E01 IP:1.4.188.72 Socket:3
DeviceType:Phone has registered.
*Apr  5 02:50:12.908: ephone-30[2]:StationSpeedDialStatReqMessage speed 4
*Apr  5 02:50:12.908: ephone-30[2]:No speed-dial set 4
*Apr  5 02:50:12.908: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:13.008: ephone-30[2]:StationSpeedDialStatReqMessage speed 3
*Apr  5 02:50:13.008: ephone-30[2]:No speed-dial set 3
*Apr  5 02:50:13.008: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:13.108: ephone-30[2]:StationSpeedDialStatReqMessage speed 2
*Apr  5 02:50:13.108: ephone-30[2]:No speed-dial set 2
*Apr  5 02:50:13.108: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:13.208: ephone-30[2]:StationSpeedDialStatReqMessage speed 1
*Apr  5 02:50:13.208: ephone-30[2]:No speed-dial set 1
*Apr  5 02:50:13.208: ephone-30[2]:StationSpeedDialStatMessage sent
*Apr  5 02:50:14.626: New Skinny socket accepted [1] (33 active)
*Apr  5 02:50:14.626: sin_family 2, sin_port 15593, in_addr 1.4.188.72
*Apr  5 02:50:14.630: skinny_add_socket 1 1.4.188.72 15593
*Apr  5 02:50:15.628: New Skinny socket accepted [1] (34 active)
*Apr  5 02:50:15.628: sin_family 2, sin_port 15693, in_addr 1.4.188.72
*Apr  5 02:50:15.628: skinny_add_socket 1 1.4.188.72 15693
*Apr  5 02:50:21.538: ephone-30[2]:SkinnyCompleteRegistration
```

Using 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 the *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.

SCCP: Configuring Analog Phone Support

Configuring Cisco Unified CME to support calls and features on analog endpoints is basically the same as configuring any SCCP phone in Cisco Unified CME. This section describes only the steps that have special meaning for SCCP analog phone support.

Prerequisites

- Cisco CME 3.2.2 or a later version for analog FXS ports on the Cisco VG 224 Voice Gateway.
- Cisco Unified CME 4.0 or a later version for analog FXS ports on the Cisco 2800 Series or Cisco 3800 Series Integrated Services Routers.

Restrictions

- FXS ports on Cisco VG 248 Analog Phone Gateways are not supported by Cisco Unified CME.
- You must set the **transfer-system** command to **full-blind** or **full-consult** to enable call transfer on analog endpoints.
- You must set the **timeouts ringing** command to **infinity** (default) on the analog ports to prevent this timeout from expiring before the ringing no-answer timeout that is configured on Cisco Unified CME with the **timeouts ringing** command in telephony-service mode.

  Note In Cisco IOS Release 12.4(11)T and later the default value of the **timeouts ringing** command is set to **infinity** for all SCCP-controlled analog ports. In releases earlier than Cisco IOS Release 12.4(11)T, the default is 180 seconds.

SUMMARY STEPS

1. Set up ephone-dns for up to 24 analog endpoints on the Cisco IOS gateway.
2. Set the maximum number of ephones.
3. Assign ephone-dns to ephones.

4. Set up feature parameters as desired.
5. Set up feature restrictions as desired.

DETAILED STEPS

Step 1 Set up ephone-dns for up to 24 endpoints on the Cisco IOS gateway.

Use the **ephone-dn** command:

```
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 that 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. Note that 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.

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 VG 224 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 setting up an ephone manually in ephone configuration mode 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.

Step 4 Set up feature parameters as desired.

- Call transfer—To use call transfer from analog endpoints, the **transfer-system** command must be configured for **full-blind** or **full-consult** in telephony-service configuration mode on the Cisco 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 Cisco Unified CME soft-key template customization command, even though analog phones do not have soft keys. Simply create a template that leaves out the soft key 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 soft-key template customization, see "Customizing Soft Keys" on page 875.

What to Do Next

- If you have SIP *and* SCCP phones connected to the same Cisco Unified CME, see the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see "SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G" on page 943.
- 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 "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

SCCP: Verifying 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.

SCCP: Enabling a 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.

Prerequisites

- 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 "Configuring Transcoding Resources" on page 323.
- A SCCP phone to be enabled as a remote phone is configured in Cisco Unified CME. For configuration information, see the "SCCP: Creating Directory Numbers" section on page 177

Restrictions

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **mtp**
5. **codec** {**g711ulaw** | **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.
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** | **g729r8** [**dspfarm-assist**]} **Example:** `Router(config-ephone)# codec g729r8 dspfarm-assist`	(Optional) Selects a preferred codec for setting up calls. • **g711ulaw**—G.711 mu-law codec (default). • **g729r8**—G.729r8 codec. • **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 the "Configuring Codec for Local Calling Between SIP and SCCP Phones" section on page 194.
- To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see "SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G" on page 943.
- 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 "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

SCCP: Verifying Remote Phones

Step 1 Use the **show running-config** command or the **show telephony-service ephone** command to verify parameter settings for remote ephones.

SCCP: Configuring Cisco IP Communicator Support

To enable support for Cisco IP Communicator, perform the following steps.

Prerequisites

- Cisco Unified CME 4.0 or a later version
- Cisco IP Communicator 2.0 or a later version
- IP address of the Cisco Unified CME TFTP server
- (Optional) Headsets with microphones for users

DETAILED STEPS

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

The download website is at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

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

Step 3 Start the Cisco IP Communicator application.

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

a. Open the Network > User Preferences window.

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

Step 5 Wait for the Cisco IP Communicator application to connect to Cisco Unified CME and register.

Step 6 Configure the extension numbers and line buttons for the Cisco IP Communicator.

Use the normal phone provisioning commands described in the "SCCP: Creating Directory Numbers" section on page 177. In the **type** command, use the **CIPC** keyword to identify this phone as a Cisco IP Communicator.

SCCP: Verifying Cisco IP Communicator Support

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

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

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

SCCP: Troubleshooting Cisco IP Communicator Support

Step 1 Use the **debug ephone detail** command to diagnose problems with calls. For more information, see the *Cisco Unified CME Command Reference*.

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.

- Configuring SCCP Phones for Making Basic Calls: Example, page 219
- Configuring SIP Phones for Making Basic Calls: Example, page 224
- Disabling a Bulk Registration for a SIP Phone: Example, page 226
- Cisco ATA: Example, page 227
- SCCP Analog Phone: Example, page 227
- Remote Teleworker Phones: Example, page 228

Configuring SCCP Phones for Making Basic Calls: Example

```
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
```

Configuring SIP Phones for Making Basic Calls: Example

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
```

Disabling a Bulk Registration for a SIP Phone: Example

The following example shows the configuration for 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
```

Cisco ATA: Example

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
```

SCCP Analog Phone: Example

The following excerpt 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 VG 224 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
!
```

Remote Teleworker Phones: Example

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
```

Where to Go Next

To select a fixed-button layout for a Cisco Unified IP Phone 7931G, see "SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G" on page 943 .

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 "Generating Configuration Files for Phones" on page 265.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Configuring Phones to Make Basic Calls

Table 11 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 11 lists the 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.

Table 11 Feature Information for Basic Call Features

Feature Name	Cisco Unified CME Versions	Feature Information
Dial Plans for SIP Phones	4.1	Dial plans for SIP phones was added.
KPML	4.1	KPML for SIP phones was added.
Session Transport Protocol	4.1	Added selection for session-transport protocol for SIP phones.
Watch Mode	4.1	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	Support for teleworker remote phones was introduced.
Analog Phones	4.0	• Support was introduced for fax pass-through mode using SCCP and a Cisco VG 224 voice gateway or Cisco ATA. • Support was introduced for analog phones with SCCP supplementary features using FXS ports on Cisco Integrated Services Routers.
	3.2.1	Support was introduced for analog phones with SCCP supplementary features using FXS ports on a Cisco VG 224 voice gateway.
	3.0	Support was introduced for Cisco ATA 186 and Cisco ATA 188.
	1.0	Support was introduced for analog phones in H.323 mode using FXS ports.
Cisco IP Communicator	4.0	Support for Cisco IP Communicator was introduced.

Table 11 Feature Information for Basic Call Features (continued)

Feature Name	Cisco Unified CME Versions	Feature Information
Direct FXO Trunk Lines	4.0	Enhancements were added 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 the 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	Direct FXO trunk line capability was introduced.
Monitor Mode for Shared Lines	3.0	Provides a visible line status indicating whether the line is in-use or not.

Creating Phone Configurations Using Extension Assigner

Last Updated: March 26, 2007

This chapter describes the Extension Assigner feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support the feature documented in this module. For a list of the versions in which this feature is supported, see the "Feature Information for Extension Assigner" section on page 263.

Contents

Prerequisites for Extension Assigner

- Cisco IOS Release 12.4(4)XC or a later release
- Cisco Unified CME 4.0(3) or a later version
- The following features must be enabled:
  - Autoassign
  - Auto-register-ephone (the default)
  - DHCP

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 Unified CME Supported Firmware, Platforms, Memory, and Voice Products* for your Cisco IOS release.
- Do not edit the Tcl script that is provided with this feature.
- When loading the Tcl script for extension assigner, you must configure it to use English as the language.

Information About Extension Assigner

To use extension assigner, you should understand the following concepts:

- Extension Assigner Overview, page 234
- Files Included in this Release, page 238

Extension Assigner Overview

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.

The documentation for this feature consists of two groups of procedures, one for installation technicians and one for system administrators. This section describes both of these sets of procedures.

Procedures for System Administrators

Before an installation technician can assign new extension numbers to phones, you must complete these procedures:

- Determine which extension numbers will be assigned to the new phones and plan your configuration.
- Download the appropriate Tcl script and associated audio prompt files and place them in the correct directory.
- 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.
   - Configure ephone-dns with the extension numbers that the installation technician can assign to phones.
   - Configure ephones 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.
- 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.

You must also determine which extension numbers to assign to the new 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 that references 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 numbers to use to reference the extension number to assign to the phone.
- What specific tag numbers to use to reference 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 assigned by the autoassign feature, and dials a specified extension number. Extension assigner requires that both the autoassign feature and autoregister feature are enabled and configured as described in earlier versions.

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 reference the extension number and must match either an ephone tag or a similar new tag called the provision-tag.

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.

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
```

If you decide to use the ephone tag, it will require less configuration. However, the installation technician will enter 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.

You do not have to configure any ephone entries for the extension number that are randomly assigned. The autoassign feature automatically creates an ephone entry for each new phone when it registers. The autoassign 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 configurations have the actual MAC address of the phone and a button with the first available ephone-dn designated for the autoassign feature.

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 autoregister feature is deleted. The number of ephone-dns that you configure for the autoassign 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 autoassign 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 purchased Cisco Unified CME phone seat 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.

Therefore, to complete the configuration, as shown in the following example, you must:

- Specify whether to use the ephone or the provision-tag number to reference 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 for each extension number that you want the installation technician to assign to a phone.
- Configure an ephone 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 more information, see the "Configuring Ephones with Temporary MAC Addresses" section on page 251.

```
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
```

Because you must configure two ephone-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 setting determines how many phones you should 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.

After you have configured your ephone and ephone-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 en 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.

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:

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 references 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.

The system administrator provides the installation technician with all of the information needed to perform this procedure.

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, you must 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

How to Configure Extension Assigner

This section consists of tasks for both the system administrator and installation technician.

Before the installation technician can use extension assigner, the system administrator must perform the following tasks:

- Determining Which Extension Numbers to Assign to the New Phones and Plan Your Configuration, page 240 (required)
- Downloading the Tcl Script, page 240 (required)
- Configuring the Tcl Script, page 241 (required)
- Specifying the Extension That Installation Technicians Call to Assign Extension Numbers, page 244 (required)
- Specifying Whether the Extension Used to Access Extension Assigner Is Dialed Automatically, page 245 (optional)
- Configuring the Extension Assigner Feature, page 246 (optional)
- Configuring Temporary Extension Numbers for Phones That Use Extension Assigner, page 247 (required)
- Configuring Extension Numbers That Installation Technicians Can Assign to Phones, page 249 (required)
- Configuring Ephones with Temporary MAC Addresses, page 251 (required)
- Configuring the Router to Automatically Save Your Configuration, page 254 (optional)
- Provide the Installation Technician with the Needed Information, page 256 (required)

The installation technician can use extension assigner to perform following tasks:

- Assigning New Extension Numbers, page 256
- Unassigning the Current Extension Number, page 257
- Reassigning the Current Extension Number, page 257

To troubleshoot your installation, see the “Verifying Extension Assigner” section on page 258.

Determining Which 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 the ephone or the provision-tag number to reference the extension number to assign to the phone.
- How many temporary extension numbers to configure. This will determine how many temporary ephone-dns and temporary MAC addresses to configure.
- What specific tag numbers to use to reference the extension number to assign to the phone.

Downloading the Tcl Script

Perform this procedure to download the Tcl script and audio prompt files for the extension assigner feature. As with all other Tcl scripts, you can download this script to a TFTP server or to the Cisco Unified CME system's flash memory. For more information about how to use Tcl scripts, see *Cisco IOS Tcl IVR and VoiceXML 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://www.cisco.com/pcgi-bin/tablebuild.pl/ip-iostsp.
2. Download the Cisco Unified CME extension assigner tar archive to a TFTP server or to the Cisco Unified CME system's flash memory.
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://www.cisco.com/pcgi-bin/tablebuild.pl/ip-iosts.	• Gives you access to Cisco Unified CME software downloads. **Note** This Web site is only available to registered Cisco.com users.
Step 2	Download the Cisco Unified CME extension assigner tar archive to a TFTP server that is accessible to the Cisco Unified CME router.	• Downloads the Cisco Unified CME extension assigner tar archive called app-cme-ea-2.0.0.0.tar (or a later version) 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 Cisco Unified CME extension assigner app-cme-ea-2.0.0.0.tar or later 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.

Configuring the Tcl Script

Perform this procedure to configure and load the Tcl script for the extension assigner feature. This procedure also specifies the password that installation technicians enter to access the extension assigner application. For more information about how to use Tcl scripts, see *Cisco IOS Tcl IVR and VoiceXML Application Guide* for your Cisco IOS release.

Note For extension assigner, you must configure the Tcl script to use English as the language.

Tip 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 tftp://10.1.1.100/app-cme-ea-2.0.0.0.tcl`	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. It can be 2 to 10 digits long.

	Command or Action	Purpose
Step 6	**paramspace english index** *number* **Example:** `Router(config-app-param)# paramspace english index 0`	Defines the category of audio files that are used for dynamic prompts by an IVR application. • *language*—Name of the language package. For the extension assigner, you must use English. • *number*—Category group of the audio files (from 0 to 4). For example, audio files representing the days and months can be category 1, audio files representing units of currency can be category 2, and audio files representing units of time—seconds, minutes, and hours—can be category 3. Range is from 0 to 4; 0 means all categories.
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. • *language*—Name of the language package. For the extension assigner, you must use English. • *prefix*—Two-character code that identifies the language associated with the audio files. For the extension assigner, you must use **en**.
Step 8	**paramspace english location** *location* **Example:** `Router(config-app-param)# paramspace english location tftp://10.1.1.100/app-cme-ea-2.0.0.0.tcl`	Defines the location of audio files that are used for dynamic prompts by an IVR application. • *language*—Name of the language package. For the extension assigner, you must use 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. • *language*—Name of the language package. For the extension assigner, you must use English. • *prefix*—Two-character code that identifies the language associated with the audio files. For the extension assigner, you must use **en**.
Step 10	**end** **Example:** `Router(config-app-param)# end`	Returns to privileged EXEC mode.

Specifying the Extension That Installation Technicians Call to Assign Extension Numbers

Perform this procedure to specify the extension number that installation technicians call to access the extension assigner application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **service** *service-name* **outbound**
5. **destination-pattern** *string*
6. **session target ipv4:***destination-address*
7. **dtmf-relay h245-alphanumeric**
8. **codec g711ulaw**
9. **no vad**
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 5999 voip`	Enters dial-peer configuration mode. • *tag*—Number used during configuration tasks to identify this dial peer.
Step 4	**service** *service-name* **outbound** **Example:** `Router(config-dial-peer)# service EA out-bound`	Loads and configures the extension assigner application on a dial peer. • *service-name*—Name that identifies the voice application. This is a user-defined name and does not have to match the script name. In this case, the name must match the name that you used to load the extension assigner Tcl script in the "Configuring the Tcl Script" section on page 241. • **outbound**—Indicates that this is an outbound dial peer. It is required for extension assigner.

	Command or Action	Purpose
Step 5	**destination-pattern** *string* **Example:** `Router(config-dial-peer)# destination pattern 5999`	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) for a dial peer. • *string*—Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. In this case, it is the extension number that the installation technician calls when assigning an extension number to a phone.
Step 6	**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 of the dial peer to receive calls. In this case, it must be the IP address for the Cisco Unified CME interface on the same router.
Step 7	**dtmf-relay h245-alphanumeric** **Example:** `Router(config-dial-peer)# dtmf-relay h245-alphanumeric`	Specifies how an H.323 or Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network. Extension assigner requires that you use **h245-alphanumeric**. • **h245-alphanumeric**—Forwards DTMF tones by using the H.245 "alphanumeric" User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.
Step 8	**codec** *codec* **Example:** `Router(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for a dial peer. • *codec*—Option that represents the correct voice decoder rate.
Step 9	**no vad** **Example:** `Router(config-dial-peer)# no vad`	Disables voice activity detection (VAD) for the calls using a particular dial peer. Extension assigner requires this.
Step 10	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Specifying Whether the Extension Used to Access Extension Assigner Is Dialed Automatically

Perform this procedure to specify whether the extension number that installation technicians call to access the extension assigner application is dialed automatically. Because this functionality should only be available for the temporary extension numbers, you should configure it only for the ephone-dns for those extensions.

This functionality is provided by the **trunk** command as described in the *Cisco Unified Communications Express Command Reference*. To see an example of how to use the **trunk** command with ephone-dns for the temporary extension numbers configured for extension assigner, see the "Configuring Temporary Extension Numbers for Phones That Use Extension Assigner" section on page 247.

Configuring the Extension Assigner Feature

Perform this procedure to specify whether to use ephone tags (the tag numbers of your ephone configurations) or provision-tags to reference the extension number. By default, the extension assigner is enabled and configured to use the ephone tag.

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. The disadvantage is that you configure an additional keyword for each ephone entry.

If you decide to use the ephone tag, it requires less configuration but the installation technician will have to enter an arbitrary tag number instead of the actual extension number when configuring a phone. This restriction is caused by the fact that 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.

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.

	Command or Action	Purpose
Step 4	**extension-assigner tag-type** {**ephone-tag** | **provision-tag**} **Example:** `Router(config-telephony)# extension-assigner tag-type provision-tag`	Specifies whether the extension assigner feature uses ephone tags (the tag numbers of your ephones configurations) or provision-tags to reference the extension number. • **ephone-tag**—Specifies that extension assigner uses the ephone tag to reference 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 uses the provision-tag to reference 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.

Configuring Temporary Extension Numbers for Phones That Use Extension Assigner

Perform this procedure to create ephone-dns to use as temporary extension numbers for any Cisco Unified CME phones to which you want the installation technician to assign extension numbers. These extensions numbers are automatically assigned to phones when they register and enable the installation technician to then assign new extension numbers.

This procedure also configures the **trunk** command to enable each extension number to automatically dial the extension assigner application.

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**

Note Repeat steps 3 to 6 for each phone.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> 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. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. • **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. **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. • *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. Unless you specify one of the optional keywords (**both** or **primary**) after the **no-reg** keyword, only the **secondary** number is not registered.
Step 5	**trunk** *digit-string* [**timeout** *seconds*] **Example:** `Router(config-ephone-dn)# trunk 9000`	(Optional) Configures the extension number to automatically dial the extension assigner application. • *digit-string*—The number of the extension assigner application. This number must match the number that you configured in "Specifying the Extension That Installation Technicians Call to Assign Extension Numbers" section on page 244 • **timeout** *seconds*—(Optional) Interdigit timeout between dialed digits, in seconds. Range is 3 to 30. Default is 3.

	Command or Action	Purpose
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. • You must follow the name order that is specified in the directory command in telephony-service configuration mode (either first-name-first or last-name-first).
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. The ephone-dn tags that you specify in this command must match the tags that you configured earlier in this procedure.
Step 10	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configuring Extension Numbers That Installation Technicians Can Assign to Phones

Perform this procedure to create ephone-dns for extensions numbers that installation technicians can assign to phones.

The readme file provided with this feature 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. **name** *name*
6. **end**

Note Repeat steps 3 to 5 for each extension number that you want to assign.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> 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. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. • **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. **Note** To change an ephone-dn from dual-line to single-line mode 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 20`	Configures a valid extension number for this ephone-dn instance. • *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. Unless you specify one of the optional keywords (**both** or **primary**) after the **no-reg** keyword, only the **secondary** number is not registered.
Step 5	**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. • You must follow the name order that is specified in the directory command in telephony-service configuration mode (either first-name-first or last-name-first).
Step 6	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

Configuring Ephones with Temporary MAC Addresses

Perform this procedure to create ephones with temporary MAC addresses for any Cisco Unified CME phones to which you want the installation technician to assign extension numbers. When the installation technician assigns a new extension number to a phone, this MAC address is overwritten by the actual MAC address of the phone. The ephone entry that was created by the extension assigner for the temporary extension number is then deleted.

You must also set the max-ephone value be at least one greater than the number of phones to which you want to assign extension numbers. This will allow the autoregister feature to automatically create at least one ephone for your temporarily extension numbers. Assuming that your max-dn setting is set high enough, your max-ephone setting determines how many phones you should 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.

Note If you want to use Cisco VG224 analog voice gateways with extension assigner, you need a minimum of 24 temporary ephones available for each gateway because they will attempt to temporary register all 24 of their ports as ephones.

You are permitted to set the max-ephone value higher than the number of purchased CME phone seat licenses is for the purpose of enrolling licensed phones using extension assigner.

The readme file provided with this feature contains some sample entries for this procedure that you can edit to fit your needs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone** *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**
8. **end**

Note Repeat steps 3 to 7 for each phone.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**`enable`** **Example:** `Router> 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 20`	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. If you use the **ephone-tag** keyword with the **extension-assigner tag-type** command, this tag is used to reference the extension number and must match the number that the installation technician enters when assigning an extension.
Step 4	**`provision-tag`** *`number`* **Example:** `Router(config-ephone)# provision-tag 20`	(Optional) Specifies a unique sequence number that is used by the extension assigner application only if you use the **provision-tag** keyword with the **extension-assigner tag-type** command. • *number*—Unique sequence number that identifies which ephone configuration and extension numbers to assign to a phone. This number must match the number that the installation technician enters when assigning an extension.
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 the extension assigner, this MAC address should begin with 02EA.EAEA. • *number*—We strongly recommends that you make this number the same as the ephone number.

	Command or Action	Purpose
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. **Note** For 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**. For Cisco CME 3.4 and earlier versions, the only type to which you can apply an add-on module is **7960**. • *phone-type*—Type **?** to display valid phone types or see the **type** command in the *Cisco Unified Communications Express Command Reference*. • *module-type*—Valid entry is the following: – **7914**—Cisco Unified IP Phone 7914 Expansion Module.
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. • *button-number*—Number of a line button on an IP phone, starting with 1 as the top 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
Step 8	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Configuring the Router to Automatically Save Your Configuration

Perform this procedure to configure the parameters for automatically saving your router configuration. If the router configuration is not saved, any extension assignments made by the installation technician will be lost when the router is restarted. We recommend that you configure your router to save your configuration every 30 minutes.

The alternative to this optional procedure is to have the installation technician connect to the router and manually issue the "write memory" command to save the router configuration.

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. • Specifies a Command Scheduler policy list.
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 specified Command Scheduler policy list. In this case, we want to save the router configuration, so the command is **write**.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-kron-policy)# exit`	Returns to global configuration mode.
Step 6	**kron occurrence** *occurrence-name* [**user** *username*] [[**in** *numdays*:]*numhours*:]*nummin* {**oneshot** | **recurring**} **Example:** `Router(config)# kron occurrence backup in 30 recurring`	Specify 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 will be created. If the occurrence-name is not new, the existing occurrence will be 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 Needed 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.
- What password to enter to access the application.
- Which tag numbers to enter to assign an extension to each phone.

Assigning New Extension Numbers

Initially, when you install your phones, they are assigned a temporary, random extension number to enable you to access extension assigner and assign new extension numbers.

Step 1 Get the information you need to use extension assigner from your system administrator. For a list of this information, see the "Provide the Installation Technician with the Needed Information" section on page 256.

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.

Step 7 If the extension is assigned to another phone that is in use, either:

- Return to Step 5 to enter another extension number.
- Perform the procedures in the "Unassigning the Current Extension Number" section on page 257 and then repeat this procedure beginning at Step 2.

Unassigning the Current 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. If this is the case, you can unassign the number so that it can be used by an another phone.

Step 1 Get the information you need to use extension assigner from your system administrator. For a list of this information, see the "Provide the Installation Technician with the Needed Information" section on page 256.

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 When you enter the ID number for the extension that is currently assigned to this phone, you are prompted to press **2** to confirm that you want to unassign the extension from the phone.

Step 6 Hang up.

Reassigning the Current Extension Number

Use this procedure if you:

- Need to replace a broken phone
- Find that you assigned the wrong number

You can reassign a new extension number to a phone if that number:

- Is not assigned to another phone
- Is assigned to another phone but the phone is currently idle or you 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 the "Provide the Installation Technician with the Needed Information" section on page 256.

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:

  a. Press **2** to confirm that you want to unassign the extension from the other phone.

  b. Hang up

  c. Perform the procedure in the "Assigning New Extension Numbers" section on page 256.

Step 7 If the extension is assigned to another phone that is in use, either:

  - Return to Step 5 to enter another extension number.

- Perform the procedures in the "Unassigning the Current Extension Number" section on page 257 and "Assigning New Extension Numbers" section on page 256.

Verifying Extension Assigner

Step 1 Use the **debug ephone extension-assigner** command to display status messages produced by the extension assigner application.

```
*Jun 9 19:08:10.627: ephone_query: inCallID=47, tag=4, ephone_tag=4
*Jun 9 19:08:10.627: extAssigner_IsEphoneMacPreset: ephone_tag = 4,
ipKeyswitch.max_ephones = 96
*Jun 9 19:08:10.627: extAssigner_IsEphoneMacPreset: ephone_ptr->mac_addr_str =
000B46BDE075, MAC_EXT_RESERVED_VALUE = 02EAEAEA0000
*Jun 9 19:08:10.627: SkinnyGetActivePhoneIndexFromCallid: callID = 47
*Jun 9 19:08:10.627: SkinnyGetActivePhoneIndexFromCallid: vdbPtr->physical_interface_type
(26); CV_VOICE_EFXS (26)
*Jun 9 19:08:10.627: SkinnyGetActivePhoneIndexFromCallid: vdbPtr->type (6);
CC_IF_TELEPHONY (6)
*Jun 9 19:08:10.627: SkinnyGetActivePhoneIndexFromCallid: htsp->sig_type (26);
CV_VOICE_EFXS (26)
*Jun 9 19:08:10.627: SkinnyGetActivePhoneIndexFromCallid: dn = 4, chan = 1
*Jun 9 19:08:10.627: ephone_query: EXTASSIGNER_RC_SLOT_ASSIGNED_TO_CALLING_PHONE
*Jun 9 19:08:22.763: ephone_unassign: inCallID=47, tag=4, ephone_tag=4
*Jun 9 19:08:22.763: extAssigner_IsEphoneMacPreset: ephone_tag = 4,
ipKeyswitch.max_ephones = 96
*Jun 9 19:08:22.763: extAssigner_IsEphoneMacPreset: ephone_ptr->mac_addr_str =
000B46BDE075, MAC_EXT_RESERVED_VALUE = 02EAEAEA000
*Jun 9 19:08:22.763: is_ephone_auto_assigned: button-1 dn_tag=4
*Jun 9 19:08:22.763: is_ephone_auto_assigned: NO
*Jun 9 19:08:22.763: SkinnyGetActivePhoneIndexFromCallid: callID = 47
*Jun 9 19:08:22.763: SkinnyGetActivePhoneIndexFromCallid: vdbPtr->physical_interface_type
(26); CV_VOICE_EFXS (26)
*Jun 9 19:08:22.767: SkinnyGetActivePhoneIndexFromCallid: vdbPtr->type (6);
CC_IF_TELEPHONY (6)
*Jun 9 19:08:22.767: SkinnyGetActivePhoneIndexFromCallid: htsp->sig_type (26);
CV_VOICE_EFXS (26)
*Jun 9 19:08:22.767: SkinnyGetActivePhoneIndexFromCallid: dn = 4, chan = 1
*Jun 9 19:08:29.795: ephone-4[8]:fStationOnHookMessage: Extension Assigner request
restart, cmd=2, new mac=02EAEAEA0004, ephone_tag=4
*Jun 9 19:08:30.063: %IPPHONE-6-UNREGISTER_NORMAL: ephone-4:SEP000B46BDE075 IP:5.5.0.1
Socket:8 DeviceType:Phone has unregistered normally.
*Jun 9 19:08:30.063: ephone-4[8][SEP000B46BDE075]:extAssigner_assign: new
mac=02EAEAEA0004, ephone-tag=4
*Jun 9 19:08:30.063: extAssigner_simple_assign: mac=02EAEAEA0004, tag=4
*Jun 9 19:08:30.063: ephone_updateCNF: update cnf_file ephone_tag=4
*Jun 9 19:08:30.063: extAssigner_assign: restart again (mac=02EAEAEA0004) ephone_tag=4
*Jun 9 19:08:30.131: %IPPHONE-6-REG_ALARM: 23: Name=SEP000B46BDE075 Load=8.0(2.0)
Last=Reset-Restart
*Jun 9 19:08:30.135: %IPPHONE-6-REGISTER_NEW: ephone-7:SEP000B46BDE075 IP:5.5.0.1
Socket:10 DeviceType:Phone has registered.
*Jun 9 19:08:30.503: %IPPHONE-6-UNREGISTER_NORMAL: ephone-7:SEP000B46BDE075 IP:5.5.0.1
Socket:10 DeviceType:Phone has unregistered normally.
*Jun 9 19:08:43.127: %IPPHONE-6-REG_ALARM: 22: Name=SEP000B46BDE075 Load=8.0(2.0)
Last=Reset-Reset
*Jun 9 19:08:43.131: %IPPHONE-6-REGISTER: ephone-7:SEP000B46BDE075 IP:5.5.0.1 Socket:13
DeviceType:Phone has registered.
```

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.

```
Jun 20 23:17:45.795: //22//TCL :/tcl_PutsObjCmd: TCL: ***** >>> app-cme-ea-2.0.0.0.tcl <<<
*****
Jun 20 23:17:45.799: //22//TCL :/tcl_PutsObjCmd: TCL: ***** >>> Cisco CME Extension
Assigner Application <<< ****
Jun 20 23:17:45.799: //22//TCL :/tcl_PutsObjCmd: >>> PROMPT: Enter password <<<
Jun 20 23:17:54.559: //22//TCL :/tcl_PutsObjCmd: >>> Collect Password Status = cd_005 <<<
Jun 20 23:17:54.563: //22//TCL :/tcl_PutsObjCmd: >>> INFO: Authentication Successful <<<
Jun 20 23:17:54.563: //22//TCL :/tcl_PutsObjCmd: >>> PROMPT: Please enter the phone tag
number  followed by the # key. Press * to re-enter the tag number <<<
Jun 20 23:17:59.839: //22//TCL :/tcl_PutsObjCmd: >>> Ephone TAG Digit Collect Status =
cd_005 <<<
Jun 20 23:17:59.843: //22//TCL :/tcl_PutsObjCmd: >>> INFO: Phone Query result = 1 <<<
Jun 20 23:17:59.843: //22//TCL :/tcl_PutsObjCmd: >>> PROMPT: Ephone Tag 6  is available
<<<
Jun 20 23:17:59.843: //22//TCL :/tcl_PutsObjCmd: >>> PROMPT: To assign extension to Phone,
press 1 to confirm, 9 to cancel <<<
Jun 20 23:17:59.851: //22//TCL :/tcl_PutsObjCmd: >>> INFO: ephone 6 is available <<<
Jun 20 23:18:20.375: //22//TCL :/tcl_PutsObjCmd: >>> INFO: TAPS Status = cd_005 <<<
Jun 20 23:18:20.379: //22//TCL :/tcl_PutsObjCmd: >>> PROMPT: Extension assignment is
successful <<<
Jun 20 23:18:20.379: //22//TCL :/tcl_PutsObjCmd: >>> INFO: Ephone extension is assigned
successfully <<<
Jun 20 23:18:28.975: //22//TCL :/tcl_PutsObjCmd: **** >>> TCL: Closing Cisco CM
```

Step 3 Use the **debug ephone state** command as described in the *Cisco IOS Debug Command Reference*.

Configuration Examples for Extension Assigner

This example for extension assigner shows a router configuration that has these 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 is not required, as 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, eleven can be plugged in one at a time. There is an exception 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
```

Additional References

The following sections provide references related to extension assigner.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	• *Cisco Unified Communications Express System Administrator Guide* • *Cisco Unified Communications Express Command Reference*
Cisco IOS voice configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference* • *Cisco IOS Debug Command Reference* • *Cisco IOS Tcl IVR and VoiceXML Application Guide*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Extension Assigner

Table 12 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 12 lists the 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.

Table 12 Feature Information for Extension Assigner

Feature Name	Cisco Unified CME Version	Feature Information
Extension Assigner	4.0(3)	Enables installation technicians to assign extension numbers to Cisco Unified CME phones without accessing the server.

Generating Configuration Files for Phones

Last Updated: March 26, 2007

This chapter describes how to generate configuration files for Cisco Unified IP phones that are connected to a Cisco Unified Communications Manager Express (Cisco Unified CME) router.

Contents

Information About Configuration Files

To generate configuration files for phones in Cisco Unified CME, you should understand the following concepts:

- Configuration Files for Phones in Cisco Unified CME, page 265
- Per-Phone Configuration Files, page 266

Configuration Files for Phones in Cisco Unified CME

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 number 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 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 the "SCCP: Defining Per-Phone Configuration Files and Alternate Location" section on page 147.

How to Generate Configuration Files for Phones

This section contains the following tasks:

- SCCP: Generating Configuration Files for SCCP Phones, page 267
- SCCP: Verifying Configuration Files for SCCP Phones, page 268
- SIP: Generating Configuration Profiles for SIP Phones, page 270
- SIP: Verifying Configuration Profiles for SIP Phones, page 271

SCCP: Generating 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.

Restrictions

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

Examples

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
```

SCCP: Verifying Configuration Files for SCCP Phones

To verify the Cisco Unified CME phone configuration, perform the following steps.

SUMMARY STEPS

1. **show telephony-service all**
2. **show telephony-service tftp-bindings**

DETAILED 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.

```
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.

```
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
```

SIP: Generating 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.

Prerequisites

- 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.
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	**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.

SIP: Verifying 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.

SUMMARY STEPS

1. **show voice register tftp-bind**
2. **show voice register profile**
3. **more system**

DETAILED STEPS

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:

```
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.

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 to be configured. See "Resetting and Restarting Phones" on page 277.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Resetting and Restarting Phones

Last Updated: March 26, 2007

This chapter describes how to reset or restart Cisco Unified IP phones that are connected to Cisco Unified Communications Manager Express (Cisco Unified CME).

Contents

Information About Resetting and Restarting Phones

Before resetting and restarting IP phones in Cisco Unified CME, you should understand the following concept:

- Differences between Resetting and Restarting IP Phones, page 277

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 13.

> **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 13 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.
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

How to 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.

This sections contains the following tasks:

- SCCP: Using the reset Command, page 279 (Required)
- SCCP: Using the restart Command, page 280 (Required)
- SIP: Using the reset Command, page 281 (Required)
- SIP: Using the restart Command, page 283 (Required)
- Verifying Basic Calling, page 284 (Optional)

SCCP: Using the reset Command

To reboot and reregister one or more SCCP phones, including contacting the DHCP server for updated information, perform the following steps.

Prerequisites

- Phones to be rebooted are connected to the Cisco Unified CME router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
   or
   ephone *phone-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.

SCCP: Using the restart Command

To fast reboot and reregister one or more SCCP phones, perform the following steps.

Prerequisites

- 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.
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.

SIP: Using the reset Command

To reboot and reregister one or more SIP phones, including contacting the DHCP server for updated information, perform the following steps.

Prerequisites

- 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 configuration mode and enters privileged EXEC mode.

SIP: Using the restart Command

To fast reboot and reregister one or more SIP phones, perform the following steps.

Prerequisites

- 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.

	Command or Action	Purpose
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.

Verifying Basic Calling

To verify that Cisco IP phones in Cisco Unified CME can place and receive calls through the voice ports, perform the following steps.

SUNNARY STEPS

1. Test local operation.
2. Test local calling area.
3. Test incoming calls.

DETAILED 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.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Configuring Dialing Plans

Last Updated: March 26, 2007

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.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Dialing Plan Features" section on page 306.

Contents

Information About Dialing Plans

To design and configure dialing plans, you should understand the following concepts:

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. For more information about types of line configurations, see "Configuring Phones to Make Basic Calls" on page 165.

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 the "Dial-Plan Patterns" section on page 289. 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 on page 290.

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 the "Direct Inward Dialing Trunk Lines" section on page 290.

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.

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

Voice translation rules perform manipulations on numbers. Voice translation profiles allow you to group voice translation rules together and associate them with the following:

- Called numbers
- Calling numbers
- Redirected called numbers

Voice translation rules have the ability to perform regular expression matches and replace substrings. The Stream Editor (SED) utility is used to translate numbers. The translation rules replace a substring of the input number if the number matches the match pattern, number plan, and type present in the rule. The SED utility is used to check for a match based on the match pattern.

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. 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 configuration information, see the "Activating a Secondary Dial Tone" section on page 303.

How to Configure Dialing Plans

This section contains the following tasks:

Dial-Plan Patterns

- SCCP: Configuring Dial-Plan Patterns, page 291 (required)
- SIP: Configuring Dial-Plan Patterns, page 292 (required)
- Verifying Dial-Plan Patterns, page 294 (optional)

Voice Translation Rules

- Defining Voice Translation Rules in Cisco CME 3.2 and Later Versions, page 295 (required)
- SCCP: Applying Voice Translation Rules in Cisco CME 3.2 and Later Versions, page 297 (required)
- SCCP: Applying Translation Rules Before Cisco CME 3.2, page 298 (required)
- SIP: Applying Voice Translation Rules in Cisco Unified CME 4.1 and Later, page 300 (required)
- SIP: Applying Voice Translation Rules before Cisco Unified CME 4.1, page 301 (required)
- Verifying Voice Translation Rules and Profiles, page 302 (optional)

Secondary Dial Tone

- Activating a Secondary Dial Tone, page 303 (optional)

SCCP: Configuring Dial-Plan Patterns

To define a dial-plan pattern, perform the following steps.

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** *extension-length* [**extension-pattern** *extension-pattern* | **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.

SIP: Configuring 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.

Prerequisites

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.

Verifying Dial-Plan Patterns

To verify dial-plan pattern configurations, perform the following steps.

SUMMARY STEPS

1. **show telephony-service**
2. **show telephony-service dial-peer**
   or
   show dial-peer summary

DETAILED STEPS

Step 1 **show telephony-service**

Use this command to verify dial-plan patterns in the configuration.

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.

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
```

Defining Voice Translation Rules in Cisco CME 3.2 and Later Versions

To define voice translation rules and voice translation profiles, perform the following steps.

Note To configure translation rules for voice calls in Cisco CME 3.1 and earlier versions, see the *Cisco IOS Voice, Video, and FAX Configuration Guide*.

Prerequisites

Cisco CME 3.2 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**} *voice-translation-rule-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 translation-rule** *number* **Example:** `Router(config)# voice translation-rule 1`	Defines a translation rule for voice calls and enters voice translation-rule configuration mode. • *number*—Number that identifies the translation rule. Range is 1 to 2147483647.

	Command or Action	Purpose
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 15. • *match-pattern*—Stream Editor (SED) expression used to match incoming call information. The slash (/) is a delimiter in the pattern. • *replace-pattern*—SED expression used to replace the match pattern in the call information. The slash (/) is a delimiter in the pattern.
Step 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**} voice-*translation-rule-tag* **Example:** `Router(cfg-translation-profile)# translate called 1`	Associates a voice translation rule with a voice translation profile. • **called**—Associates the translation rule with called numbers. • **calling**—Associates the translation rule with calling numbers. • **redirect-called**—Associates the translation rule with redirected called numbers. • *translation-rule-tag*—Reference number of the translation rule. Range is 1 to 2147483647.
Step 8	**end** **Example:** `Router(cfg-translation-profile)# end`	Exits configuration mode and enters 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 the "SCCP: Applying Voice Translation Rules in Cisco CME 3.2 and Later Versions" section on page 297.
- To apply voice translation profiles to SIP phones connected to Cisco Unified CME 4.1 or a later version, see the "SIP: Applying Voice Translation Rules in Cisco Unified CME 4.1 and Later" section on page 300.
- To apply voice translation profiles to SIP phones connected to Cisco Unified CME 3.4 or Cisco Unified 4.0(x), see the "SIP: Applying Voice Translation Rules before Cisco Unified CME 4.1" section on page 301.

SCCP: Applying Voice Translation Rules in Cisco CME 3.2 and Later Versions

To apply a voice translation profile to modify the number dialed by extensions on a SCCP phone, perform the following steps.

Prerequisites

- 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 the "Defining Voice Translation Rules in Cisco CME 3.2 and Later Versions" section on page 295.

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.

	Command or Action	Purpose
Step 4	**translation-profile** {**incoming** | **outgoing**} *name* **Example:** `Router(config-ephone-dn)# translation-profile outgoing name1`	Assigns a translation profile for incoming or outgoing call legs to or from Cisco Unified IP phones. • 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(config-ephone-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 "Generating Configuration Files for Phones" on page 265.

SCCP: Applying Translation Rules Before Cisco 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.

Prerequisites

Translation rule to be applied must be already configured by using the **translation-rule** and **rule** commands. For configuration information, see the *Cisco IOS Voice, Video, and FAX Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **translate** {**called** | **calling**} *translation-rule-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-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 "Generating Configuration Files for Phones" on page 265.

SIP: Applying Voice Translation Rules in Cisco Unified CME 4.1 and Later

To apply a voice translation profile for incoming call legs to a directory number on a SIP phone, perform the following steps.

Prerequisites

- 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 the "Defining Voice Translation Rules in Cisco CME 3.2 and Later Versions" section on page 295.

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-register-dn)# ephone-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-ephone-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 "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

SIP: Applying Voice Translation Rules 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.

Prerequisites

- Cisco CME 3.4 or a later version.
- Voice translation rule to be applied must be already configured. For configuration information, see the "Defining Voice Translation Rules in Cisco CME 3.2 and Later Versions" section on page 295.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register 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 "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

Verifying Voice Translation Rules and Profiles

To verify voice translation profiles, and rules, perform the following steps.

SUMMARY STEPS

1. **show voice translation-profile**
2. **show voice translation-rule**
3. **test voice translation-rule**

DETAILED STEPS

Step 1 **show voice translation-profile** [*name*]

This command displays the configuration of one or all translation profiles.

```
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.

```
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.

```
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
```

Activating a Secondary Dial Tone

To activate a secondary dial tone after a phone user dials the specified number string, perform the following steps.

Prerequisite

- 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.

	Command or Action	Purpose
Step 4	**secondary-dialtone** *digit-string* **Example:** `Router(config-telephony)#` **`secondary-dialtone 9`**	Activates a secondary dial tone when *digit-string* is dialed. • *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.

Configuration Examples for Dialing Plan Features

This section contains the following example:

- Secondary Dial Tone: Example, page 304

Secondary Dial Tone: Example

```
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
!
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Dialing Plan Features

Table 14 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 14 lists the 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.

Table 14 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.
Secondary Dial Tone	3.0	Support for secondary dial tone after dialing specified number string.
Voice Translation Rules	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.

Configuring Localization Support

Last Updated: September 13, 2007

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.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Localization Support" section on page 323.

Contents

Information About Localization

To configure localization support, you should understand the following concepts:

System-Defined Locales

Cisco Unified CME provides built-in 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 7906, 7911, 7941, 7961, 7970, and 7971—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 the "Installing System-Defined Locales for Cisco Unified IP Phone 7906, 7911, 7941, 7961, 7970, and 7971" section on page 310.

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, 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: http://www.loc.gov/standards/iso639-2/. User-defined country codes for network locales are based on ISO 3166 codes.

For configuration information, see the "Installing User-Defined Locales" section on page 313.

Localization Support for Phone Displays

On the Cisco Unified IP Phone 7906, 7911, 7941, 7961, 7970, and 7971, 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
- Soft keys (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 4.0 and later, 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 the "Configuring Multiple Locales" section on page 316.

How to Configure Localization Support

This section contains the following tasks:

- Installing System-Defined Locales for Cisco Unified IP Phone 7906, 7911, 7941, 7961, 7970, and 7971, page 310 (required)
- Installing User-Defined Locales, page 313 (optional)
- Verifying User-Defined Locales, page 315 (optional)
- Configuring Multiple Locales, page 316 (optional)
- Verifying Multiple Locales, page 319 (optional)

Installing System-Defined Locales for Cisco Unified IP Phone 7906, 7911, 7941, 7961, 7970, and 7971

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.

Prerequisites

- Cisco Unified CME 4.0(2) or a later version.
- You must create per-phone configuration files as described in the "SCCP: Defining Per-Phone Configuration Files and Alternate Location" section on page 147.

Restrictions

- Localization is not supported for SIP phones.
- Cisco Unified IP Phone 7931G supports United States English only.
- 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.

DETAILED STEPS

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 **Cancel** at the login dialog box and follow the instructions that appear.

Step 2 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*

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, slot 0, or an external TFTP server.

```
Router# archive tar /xtract source-url flash:/file-url
```

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 15 and Table 16 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

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 15 Phone-Type Codes for Locale JAR Files

Phone Type	Phone Code
7906/7911	tc
7941/7961	mk
7970/7971	td

Table 16 System-Defined User and Network Locales

Language	Language Code	User-Locale Directory Name	Country Code	Network-Locale Directory Name
English	en	English_United_States[1]	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
Italian	it	Italian_Italy	IT	Italy
Japanese[2]	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

1. 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.
2. 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 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:

```
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 16 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 16 and remove the two-letter language code from the JAR file name.

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 to use special phrases.

- Only flash 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 the "Configuring Multiple Locales" section on page 316.

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.

Installing 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.

Prerequisites

- Cisco Unified CME 4.0(3) or a later version.
- You must create per-phone configuration files as described in the "SCCP: Defining Per-Phone Configuration Files and Alternate Location" section on page 147.

Restrictions

- Localization is not supported for SIP phones.
- 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.

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

Step 2 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*

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, or an external TFTP server.

```
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 Phones 7905, 7912, 7940, or 7960, go to Step 11.
For Cisco Unified IP Phones 7911, 7941, 7961, 7970, or 7971, go to Step 7.

Step 7 Each phone type has a JAR file that uses the following naming convention:

language-*type*-sccp.jar

For example, zh-td-sccp.jar is Traditional Chinese for the Cisco Unified IP Phone 7970.

See Table 17 and Table 18 for a description of the codes used in the filenames.

Table 17 Phone-Type Codes for Locale Files

Phone Type	Code
7906/7911	tc
7941/7961	mk
7970/7971	td

Table 18 Language Codes for User-Defined Locales

Language	Language Code
Bulgarian	bg
Chinese	zh
Finnish	fi
Hungarian	hu
Korean	ko
Polish	pl

Step 8 If you store the locale files in flash or slot 0: on the Cisco Unified CME router, create a TFTP alias using this format:

```
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

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.

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.

```
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, slot 0, or an external TFTP server. Rename the files using the format user_define_*number*_*filename* where *number* is 1 to 5. 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, 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 the "Configuring Multiple Locales" section on page 316.

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.

Verifying User-Defined Locales

See the "Verifying Multiple Locales" section on page 319.

Configuring Multiple Locales

To define one or more alternatives to the default user and network locales, and apply them to individual phones, perform the following steps.

Prerequisites

- 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 the "SCCP: Defining Per-Phone Configuration Files and Alternate Location" section on page 147.
- You can also use user-defined locale codes as alternative locales after you download the appropriate XML files. See the"Installing User-Defined Locales" section on page 313.

Restrictions

- 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 Station 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **user-locale** *user-locale-tag* [*user-defined-code*] *language-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** **Example:** `Router> 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	**user-locale** *user-locale-tag* [*user-defined-code*] *language-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 language code. Range is 0 to 4. This argument is required when using multiple locales; otherwise the specified language is the default applied to all phones. • *user-defined-code*—(Optional) Assigns one of the user-defined codes to the specified language code. Valid codes are **U1**, **U2**, **U3**, **U4**, and **U5**. • *language-code*—Type **?** to display a list of system-defined codes. United States (US) is the default. 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. This argument is required when using multiple locales; otherwise the specified country is the default applied to all phones. • *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. United States (US) is the default. 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. 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. 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.

Verifying Multiple Locales

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.

```
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.

Configuration Examples for Localization

This section contains the following examples:

- Multiple User and Network Locales: Example, page 320
- User-Defined Locales: Example, page 321

Multiple User and Network Locales: Example

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
```

User-Defined Locales: Example

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
```

Where to Go Next

Ephone Templates

For more information about ephone templates, see "Creating Templates" on page 927.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Localization Support

Table 19 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 19 lists the 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.

Table 19 Feature Information for Localization Support

Feature Name	Cisco Unified CME Version	Feature Information
Multiple Locales	4.0	Support for multiple user and network locales was introduced.
User-Defined Locales	4.0	User-defined locales were introduced.

Configuring Transcoding Resources

Last Updated: June 18, 2007

This chapter describes the transcoding support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Transcoding Resources" section on page 357.

Contents

Prerequisites for Transcoding Resources

- Cisco Unified CME 3.2 or a later version.
- Cisco Unified CME routers and external voice routers on the same LAN must be configured with digital signal processors (DSPs) that support transcoding.
- 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.

Restrictions for Transcoding Resources

- Versions earlier than Cisco CME 3.2 support only G.729 for two-party voice calls.
- Transcoding between G.711 and G.729 does not support the following:
  - Meet-me conferencing
  - Multiple-party conferencing
  - Transcoding security

Information About Transcoding Resources

To configure transcoding support, you should understand the following concepts:

- Transcoding Support, page 324
- Transcoding When a Remote Phone Uses G.729r8, page 325
- Secure DSP Farm Transcoding, page 326

Transcoding Support

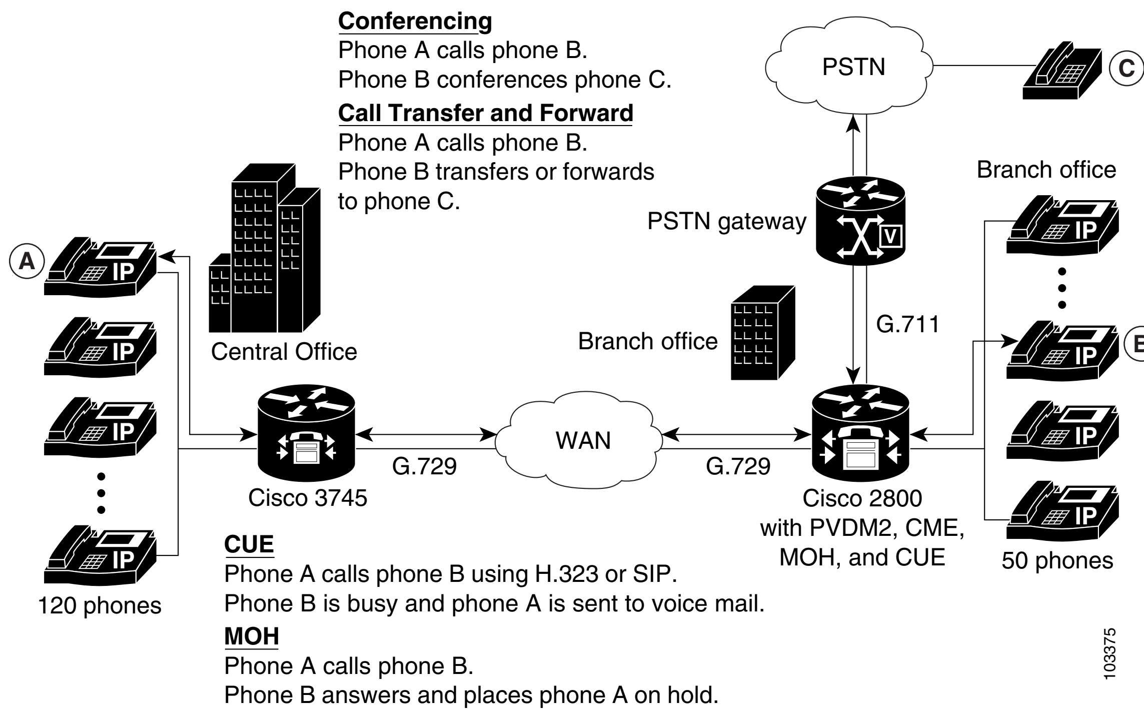
Transcoding compresses and decompresses voice streams to match endpoint-device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth, and the local device does not support that type of compression.

Cisco 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—An H.323 or SIP call using G.729 is forwarded to Cisco Unity Express. Cisco Unity Express supports only G.711, so G.729 must be transcoded. See the Cisco Unity Express documentation at www.cisco.com/en/US/products/sw/voicesw/ps5520/tsd_products_support_series_home.html
- Music on hold (MOH)—The phone receiving MOH is part of a system that uses G.729. The G.711 MOH is transcoded into G.729 resulting in a poorer quality sound due to the lower compression of G.729.

Figure 14 provides an example of each of the four call situations described.

Figure 14 Three-Way Conferencing, Call Transfer and Forward, Cisco Unity Express, and MOH Between G.711 and G.729



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 the "Transcoding When a Remote Phone Uses G.729r8" section on page 325. 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.

How to Configure Transcoding Resources

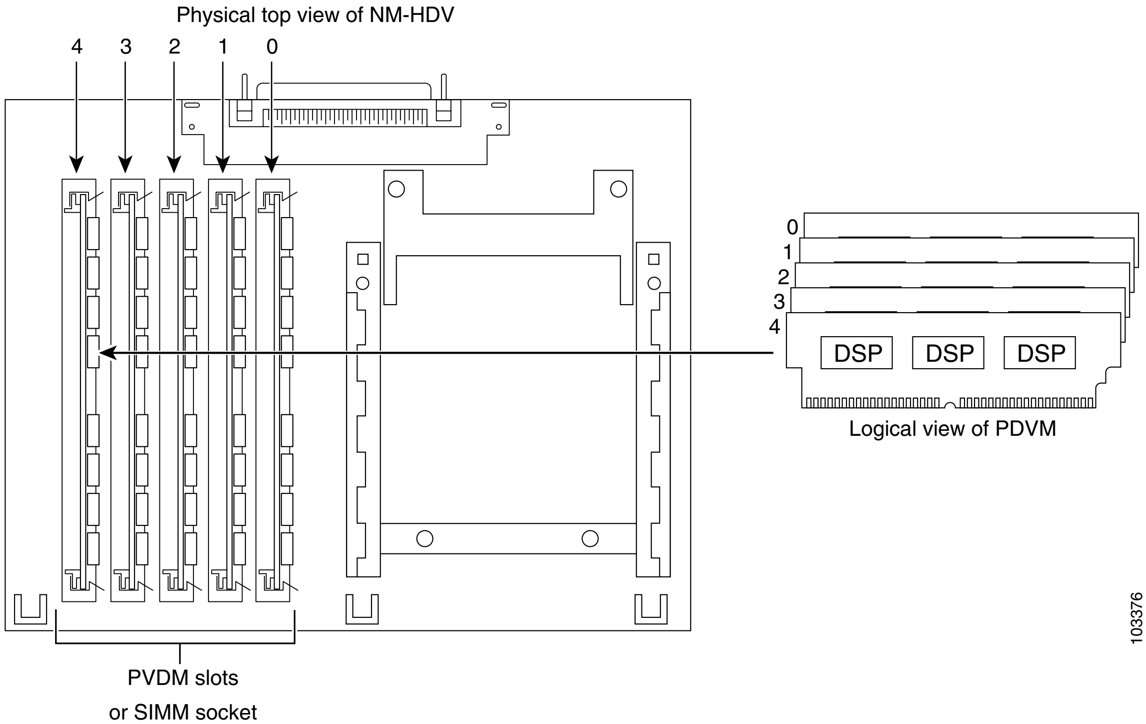
This section contains the following tasks:

Determining DSP Resources for Transcoding

Transcoding is facilitated through DSPs, which are located in network modules. All network modules have single inline 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.

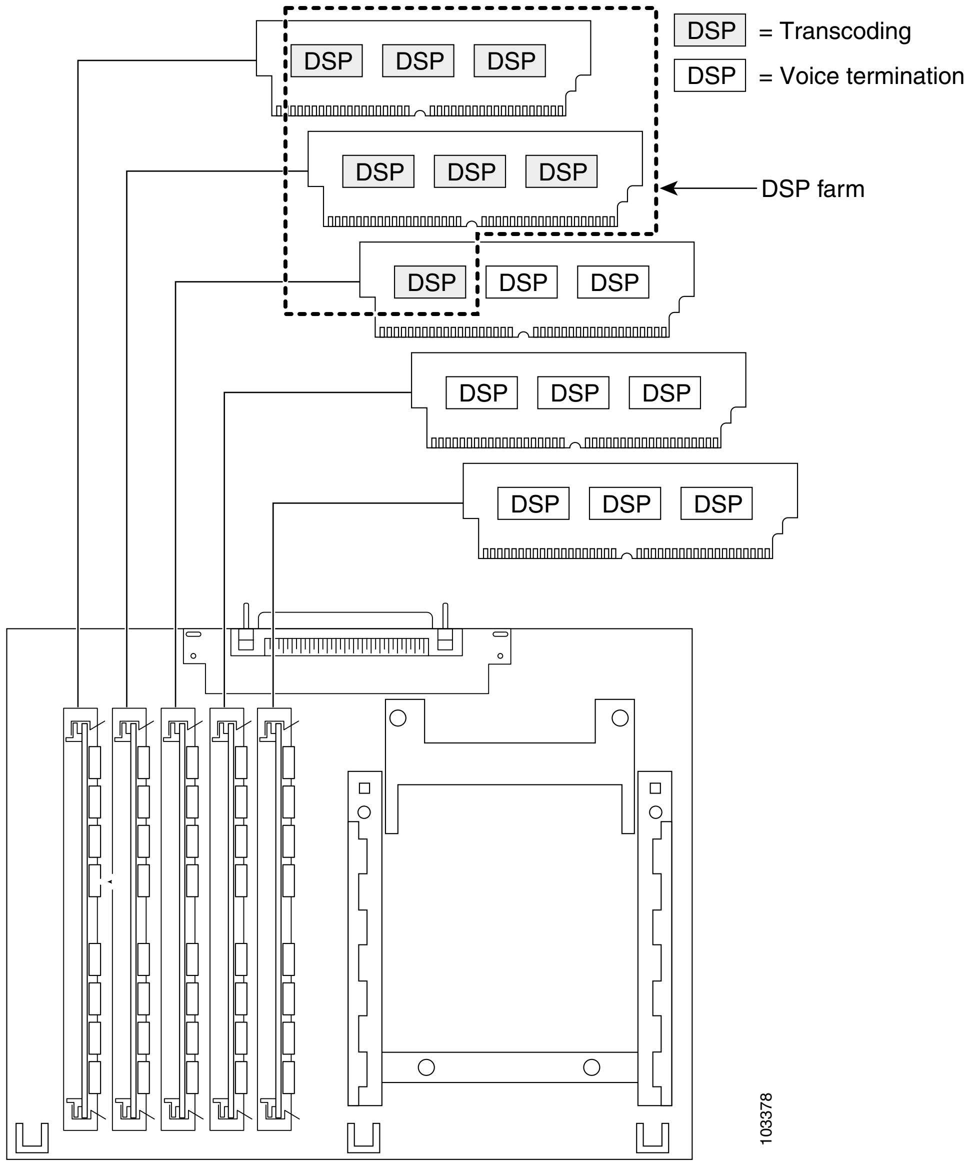
Figure 15 shows an NM-HDV with five SIMM sockets or PVDM slots that each hold a 12-Channel PVDM (PVDM-12). Each PVDM-12 holds three TI 549 DSPs. Each DSP supports four channels.

Figure 15 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 16 shows a DSP farm managed by Cisco Unified CME.

Figure 16 DSP Farm



Note 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.

To determine how many DSP voice resources are on your Cisco Unified CME router, use the **show voice dsp** command. To determine how many DSP farms have been configured, use the **show sdspfarm sessions** and **show sdspfarm units** commands. For more information about these commands, see the *Cisco Unified Communications Manager Express Command Reference*.

For information on determining if your router has the correct DSP allocation for transcoding, see the "Allocation of DSP Resources" section in the "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" chapter of the *Cisco Unified Communications Manager and Cisco IOS Interoperability Guide*.

Provisioning NMs or NM Farms for Transcoding

To provision NMs or NM farms for transcoding, you must determine the required number of PVDMs and install them in either NMs or NM farms. A single NM holds up to five PVDMs. On routers capable of holding multiple devices, NMs or NM farms can be allocated to support different functionalities.

Step 1 Determine performance requirements.

Step 2 Determine the number of transcoding sessions that your router must support.

Step 3 Determine the number of DSPs that are required.

From Table 8 or Table 9 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*, determine the number of DSPs that are required to support the transcoding sessions. Note that Cisco Unified CME does not support DSP-farm conferencing, so only the transcoding portion of this discussion applies to Cisco Unified CME. If voice termination is required in addition, determine the additional number of required DSPs from the tables. For example, 16 transcoding sessions (30-ms packetization) and 4 G.711 voice calls require two DSPs.

Step 4 Determine the number of DSPs that are supportable.

From Table 4 in the "Allocation of DSP Resources" section of the "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" chapter of the *Cisco CallManager and Cisco IOS Interoperability Guide*, determine the maximum number of NMs or NM farms that your router can support.

Step 5 Verify your solution.

Ensure that your requirements fall within router capabilities, taking into account whether your router supports multiple NMs or NM farms. If necessary, reassess performance requirements.

Step 6 Install hardware to prepare your system for DSP-farm configuration.

Install PVDMs, NMs, and NM farms as needed.

What to Do Next

Choose from one of the following options:

- To set up DSP farms for NM-HDVs, see the "Configuring DSP Farms for NM-HDVs" section on page 334.
- To set up DSP farms on NM-HDs and NM-HDV2s, see the "Modifying the Number of Transcoding Sessions for NM-HDVs" section on page 336.

Configuring DSP Farms for NM-HDs and NM-HDV2s

To configure DSP farms for NM-HDs or NM-HDV2s and to configure secure transcoding profiles, perform the following procedure.

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**
12. **associate profile** *profile-identifier* **register** *device-name*
13. **keepalive retries** *number*
14. **switchover method** {**graceful** | **immediate**}
15. **switchback 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.
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`	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 priority 2`	Specifies the Cisco Unified CME address. • *ip-address*—IP address of the Cisco Unified CME server. • **identifier** *identifier-number*—Identifier used to associate the SCCP Cisco Unified CME IP address with a Cisco Unified CME group. See the **associate ccm** command in Step 11. • Repeat this step to specify the address of a secondary Cisco Unified CME server.
Step 8	**`sccp`** **Example:** `Router(config)# sccp`	Enables SCCP and its associated transcoding and conferencing applications.

	Command or Action	Purpose
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. Range is 1 to 65535. There is no default value. **Note** A Cisco Unified CME group is a naming device under which data for the DSP farms is declared. Only one group is required. For the Cisco Unified CME group you must assign a priority to the group, associate the group with a DSP farm profile, and set the keepalive, switchback, and switchover parameters.
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** **Example:** `Router(config-sccp-ccm)# associate ccm 1 priority`	Associates a Cisco Unified CME with a group and establishes its priority within the group. • *identifier-number*—Number that identifies Cisco Unified CME. Range is 1 to 65535. There is no default value. • **priority**—The priority of the Cisco Unified CME router in the Cisco Unified CME group. The default is 1 because only one Cisco Unified CME group is possible. • Repeat this step to associate a secondary Cisco Unified CME server with a group.
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. Range is 1 to 65535. There is no default value. • **register** *device-name*—User-specified device name in Cisco Unified CME. The *device-name* must use the format of mtp *mac-address*, 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 is 1 to 32. The default is 3.

	Command or Action	Purpose
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	**switchback 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. • **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 is 60 to 172800. Default is 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 is 60 to 172800. Default is 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 is 1 to 3600. Default is 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 is 1 to 65535. There is no default. • **transcode**—Enables profile for transcoding. • **security**—Enables profile for secure DSP farm services.
Step 19	**trustpoint** *trustpoint-label* **Example:** `Router(config-dspfarm-profile)# trustpoint dspfarm`	(Optional) Associates a trustpoint with a DSP farm profile.

	Command or Action	Purpose
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. • Use CLI help to locate a list of codecs. • Repeat this step as necessary to specify all the supported codecs.
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 is 0 to X. Default is 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.

Configuring DSP Farms for NM-HDVs

To configure DSP farms for NM-HDVs, perform the following steps.

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. **dspfarm 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 server. • **priority** *priorit*y—Priority of the Cisco Unified CME server relative to other connected servers. Range is 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	**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. 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.

Modifying the Number of Transcoding Sessions for NM-HDVs

To modify the maximum number of transcoding sessions for NM-HDVs, perform the following steps.

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.

	Command or Action	Purpose
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.

Configuring the Cisco Unified CME Router to Act as the DSP Farm Host

To configure the Cisco Unified CME router to act as the DSP farm host, perform the following tasks.

- Determining the Maximum Number of Transcoder Sessions, page 337
- Setting the Cisco Unified CME Router to Receive IP Phone Messages, page 338
- Configuring the Cisco Unified CME Router to Host a Secure DSP Farm, page 340

Determining the Maximum Number of Transcoder Sessions

To determine the maximum number of transcoder sessions that can occur at one time perform the following steps.

SUMMARY STEPS

1. **dspfarm transcoder maximum sessions**
2. **show sdspfarm sessions**
3. **show sdspfarm units**
4. Determine maximum number of transcoder sessions based on values in steps 2 and 3.

DETAILED 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.

Step 3 Use the **show sdspfarm units** command to display the number of DSP farms.

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.

Setting the Cisco Unified CME Router to Receive IP Phone Messages

To set the Cisco Unified CME router to receive IP phone messages and to set the maximum number of DSP farms and transcoder sessions, perform the following steps.

Note You can unregister all active calls' transcoding streams with the **sdspfarm unregister force** command.

Prerequisites

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 as shown in the following output:

```
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)
```

The MAC address of the Fast Ethernet interface is 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-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	**`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`**`]` **Example:** `Router(config-telephony)# ip source address 10.10.10.1 port 3000`	Enables a router to receive messages from Cisco Unified IP phones through the router's IP addresses and ports. • *address*—The range is 0 to 5. The default is 0. • **port** *port*—(Optional) TCP/IP port used for SCCP. The default is 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 server. • *number*—The range is 0 to 5. The default is 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*—Range is 0 to 128. Default is 0. **Note** For the value of *number*, you can use the value obtained in step 4 in the "Determining the Maximum Number of Transcoder Sessions" section on page 337.

	Command or Action	Purpose
Step 7	**sdspfarm tag** *number device-name* **Example:** `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. • *number*—The tag number. The range is 1 to 5. • *device-name*—The 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.

Configuring the Cisco Unified CME Router to Host a Secure DSP Farm

You must configure the Media Encryption Secure Real-Time Transport Protocol (SRTP) feature on the Cisco Unified CME router, making it a secure Cisco Unified CME, before it can host a secure DSP farm. See "Configuring Security" on page 409 for information on configuring a secure Cisco Unified CME.

Registering the DSP Farm with Cisco Unified CME 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.

This section contains the following tasks:

- Obtaining a Digital Certificate from a CA Server, page 340
- Copying the CA Root Certificate of the DSP Farm Router to the Cisco Unified CME Router, page 346
- Copying the CA Root Certificate of the Cisco Unified CME Router to the DSP farm Router, page 347
- Configuring Cisco Unified CME to Allow the DSP Farm to Register, page 347
- Verifying DSP Farm Registration with Cisco Unified CME, page 348

Obtaining a 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.

This section contains the following tasks:

- Configuring a CA Server, page 341 (Optional)
- Creating a Trustpoint, page 343
- Authenticating and Enrolling the Certificate with the CA Server, page 345

Configuring a CA Server

Note Skip this procedure if the DSP farm resides on the same router as the Cisco Unified CME. Proceed to the "Creating a Trustpoint" section on page 343.

The CA server automatically creates a trustpoint where the certificates are stored. The automatically created trustpoint stores the CA root certificate.

Prerequisites

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. **crypto pki trustpoint** *label*
9. **revocation-check crl**
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.
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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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. The label **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.
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.

Creating a Trustpoint

The trustpoint stores the digital certificate for the DSP farm. To create a trustpoint, perform the following procedure:

Prerequisites

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.
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 phone's.

	Command or Action	Purpose
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.

Authenticating and Enrolling the Certificate with the CA Server

Prerequisites

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.

	Command or Action	Purpose
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 "Creating a Trustpoint" section on page 343.
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 "Creating a Trustpoint" section on page 343.

Copying 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.

Prerequisites

Cisco Unified CME 4.2 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
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.

	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. **Note** The *label* is the trustpoint label specified in the "Creating a Trustpoint" section on page 343.
Step 4	**enrollment terminal** **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment.
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.

Copying the CA Root Certificate of the Cisco Unified CME Router to the DSP farm Router

Repeat the steps in the "Copying the CA Root Certificate of the DSP Farm Router to the Cisco Unified CME Router" section on page 346 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.

Configuring Cisco Unified CME to Allow the DSP Farm to Register

Prerequisites

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 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 17 of the "Configuring DSP Farms for NM-HDs and NM-HDV2s" section on page 330.
Step 7	**`exit`** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.

Verifying 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: Example

```
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: Example

```
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
```

Verifying DSP Farm Operation

To verify that the DSP farm is registered and running, perform the following steps in any order.

SUMMARY STEPS

1. **show sccp** [**statistics** | **connections**]
2. **show sdspfarm units**
3. **show sdspfarm sessions**
4. **show sdspfarm sessions summary**
5. **show sdspfarm sessions active**

6. **show sccp connections details**
7. **debug sccp** {**all** | **errors** | **events** | **packets** | **parser**}
8. **debug dspfarm** {**all** | **errors** | **events** | **packets**}
9. **debug ephone mtp**

DETAILED STEPS

Step 1 Use the **show sccp** [**statistics** | **connections**] command to display the SCCP configuration information and current status.

```
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.

```
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.

```
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.

```
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.

```
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.

```
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.

Tuning DSP Farm Performance

To tune DSP farm performance, perform the following steps.

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.

Configuration Examples for Transcoding Resources

This section contains the following examples:

- DSP Farms for NM-HDVs: Example, page 354
- DSP Farms for NM-HDs and NM-HDV2s: Example, page 354
- Cisco Unified CME Router as the DSP Farm Host: Example, page 355

DSP Farms for NM-HDVs: Example

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
```

DSP Farms for NM-HDs and NM-HDV2s: Example

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 g719abr8
 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
```

Cisco Unified CME Router as the DSP Farm Host: Example

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
```

Where to go Next

Music on Hold

Music on hold can require transcoding resources. See "Configuring Music on Hold" on page 817.

Teleworker Remote Phones

Transcoding has benefits and disadvantages for remote teleworker phones. See the discussion in "Configuring Phones to Make Basic Calls" on page 165.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Transcoding Resources

Table 20 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 20 lists the 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.

Table 20 Feature Information for Transcoding Resources

Feature Name	Cisco Unified CME Version	Feature Information
Transcoding Support	3.2	Transcoding between G.711 and G.729 was introduced.
Secure Transcoding	4.2	Secure transcoding for calls using the **codec g729r8 dspfarm-assist** command was introduced.

Enabling the GUI

Last Updated: June 18, 2007

This chapter describes the Cisco Unified Communications Manager Express (Cisco Unified CME) graphical user interface (GUI) and explains how to set it up for three different levels of user.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Enabling the GUI" section on page 374.

Contents

Prerequisites for Enabling the GUI

GUI files must be copied into flash memory on the router. For information about files, see "Installing and Upgrading Cisco Unified CME Software" on page 87.

Restrictions for Enabling the GUI

- 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. If you are downgrading or upgrading your Cisco Unified CME version, you must downgrade or upgrade your GUI files. For information, see "Installing and Upgrading Cisco Unified CME Software" on page 87.
- 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 will result in a long delay before results are shown.

Information About Enabling the GUI

To enable GUI support, you should understand the following concepts:

- Cisco Unified CME GUI Support, page 360
- AAA Authentication, page 361

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.

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 CLI 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 the "Configuring Authentication" chapter of the *Cisco IOS Security Configuration Guide* for your Cisco IOS release.

How to Enable the GUI

This section contains the following procedures:

- Enabling the HTTP Server, page 361 (required)
- Enabling GUI Access for the System Administrator, page 363 (required)
- Accessing the Cisco Unified CME GUI, page 364 (required)
- Creating a Customized XML File for Customer Administrator GUI, page 365 (optional)
- Enabling GUI Access for Customer Administrators, page 366 (optional)
- Enabling GUI Access for Phone Users, page 368 (optional)
- Troubleshooting the Cisco Unified CME GUI, page 369 (optional)

Enabling 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.
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.

Enabling 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*—System administrator username. 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, the **time-webedit** command can be used 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.

Accessing the Cisco Unified CME GUI

To access the Cisco Unified CME router through the GUI to make configuration changes, perform the following steps.

Restrictions

The Cisco Unified CME GUI requires Microsoft Internet Explorer 5.5 or a later version. Other browsers are not supported.

DETAILED STEPS

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
```

Step 2 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 3 After you login and are authenticated, the system displays one of the following home pages, based on your user level:

- The system administrator home page.
- The 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.
- The phone user home page.

After you log in successfully, online help is available from the Help menu.

Creating 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 *Cisco IP Phone Services Application Development Notes*. This template is one of the Cisco Unified CME files that you download from the Cisco Software Center during installation.

To edit and load the XML configuration file, perform the following steps.

SUMMARY STEPS

1. Copy the XML template and open it in any text editor.
2. Edit the XML template.
3. Copy the file to a TFTP or FTP server that can be accessed by the Cisco Unified CME router.
4. Copy your file to flash memory on the Cisco Unified CME router.
5. Load the XML file from router flash memory.

DETAILED STEPS

Step 1 Copy the XML template that you downloaded from the Cisco Software Center and open it in any text editor (see the "XML Configuration File Template: Example" section on page 370). Give the file a name that is meaningful to you and that uses "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.

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 "XML Configuration File: Example" section on page 371.

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.

```
Router# copy tftp flash
```

Step 5 Load the XML file from router flash memory.

```
Router(config)# telephony-service
Router(config-telephony)# web customize load filename
Router(config-telephony)# exit
```

Enabling GUI Access for Customer Administrators

Perform one of the following procedures to enable GUI access for a customer administrator, depending on the method you want to use:

- Using the Cisco Unified CME GUI to Define a Customer Administrator Account, page 366
- Using the Cisco IOS CLI to Define a Customer Administrator Account, page 367

Prerequisites

- Enable a system administrator account for GUI access. See the "Enabling GUI Access for the System Administrator" section on page 363.
- Create the XML configuration file for the customer administrator GUI. See the "Creating a Customized XML File for Customer Administrator GUI" section on page 365.
- Reload the XML file using the **web customize load** command if you have made changes to the customer administrator GUI.

Using the Cisco Unified CME GUI to Define a Customer Administrator Account

To allow the system administrator to use the GUI to create a customer administrator account, perform the following steps.

DETAILED STEPS

Step 1 From the Configure System Parameters menu, choose **Administrator's Login Account**.

Step 2 Complete the Admin User Name (username), Admin User Type (Customer), and New Password fields for the user that you are defining as a customer administrator. Type the password again to confirm it.

Step 3 Click **Change** for your changes to become effective.

Using the Cisco IOS CLI to Define a Customer Administrator Account

To allow the system administrator to create a customer administrator account by using the Cisco IOS CLI, 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.
Step 3	**`telephony-service`** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
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. The default username is Customer. There is no default password. • **name** *username*—Username of customer administrator. • **password** *string*—String to verify customer administrator identity.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Enabling GUI Access for Phone Users

Perform one of the following procedures to enable GUI access for a phone user, depending on the method you want to use:

- Using the Cisco Unified CME GUI to Define a Phone User Account, page 368
- Using the Cisco IOS CLI to Define a Phone User Account, page 369

Prerequisites

- Enable a system administrator account for GUI access. See the "Enabling GUI Access for the System Administrator" section on page 363.

Using the Cisco Unified CME GUI to Define a Phone User Account

To create a phone user account by using the Cisco Unified CME GUI, perform the following steps.

DETAILED 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 displays.

Step 2 Enter a username and password in the **Login Account** area of the screen. If you are adding a new phone, complete the other fields as appropriate.

Step 3 Click **Change** for your edits to become effective.

Using the Cisco IOS CLI to Define a Phone User Account

To create a GUI account for a phone user by using the Cisco IOS CLI, perform the following steps.

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

Troubleshooting the Cisco Unified CME 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 called cme-3.2.0-gui.tar (or a later version of the file) to ensure that you have the most recent files installed in flash memory. The latest version can be downloaded from the Cisco Unified CME Software Download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Configuration Examples for Enabling the GUI

This section contains the following examples:

HTTP and Account Configuration: Example

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
```

XML Configuration File Template: Example

```
<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>
```

XML Configuration File: Example

```
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>
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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 Security Command Reference* • *Cisco IOS Software Releases 12.4T Command References*

Related Topic	Document Title
Cisco IOS configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Security Configuration Guide* • *Cisco IOS Software Releases 12.4T Configuration Guides*
Phone documentation for Cisco Unified CME	• *Quick Reference Cards* • *User Guides*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Enabling the GUI

Table 21 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The following table lists the 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.

Table 21 Feature Information for Enabling the GUI

Feature Name	Cisco Unified CME Version	Feature Information
Cisco Unified CME GUI	2.0	The Cisco Unified CME GUI was introduced.

Integrating Voice Mail

Last Updated: September 5, 2007

This chapter describes how to integrate your voice-mail system with Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Voice-Mail Integration" section on page 407.

Contents

Prerequisites

- Calls can be successfully completed between phones on the same Cisco Unified CME router.
- If your voice-mail system is something other than Cisco Unity 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/ps3115/prod_installation_guides_list.html.
- The recommended Cisco IOS release and feature set plus the necessary Cisco CME phone firmware and GUI files to support Cisco Unity Express are installed on the Cisco CME router.

  If the GUI files are not installed, see the "Installing Cisco Unified CME Software" section on page 92.

  To determine whether the Cisco IOS software release and Cisco CME software version are compatible with the Cisco Unity Express version, Cisco router model, and Cisco Unity Express hardware that you are using, see the 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/products/sw/voicesw/ps5520/products_documentation_roadmap09186a00803f3e19.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/products/sw/voicesw/ps5520/products_documentation_roadmap09186a00803f3e19.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/products/sw/voicesw/ps5520/products_documentation_roadmap09186a00803f3e19.html.

Information About Voice-Mail Integration

To enable voice-mail support, you should understand the following concepts:

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 the *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 the "Enabling DTMF Integration Using SIP NOTIFY" section on page 393.

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 the "Enabling DTMF Integration Using RFC 2833" section on page 390.

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 the "Enabling DTMF Integration for Analog Voice-Mail Applications" section on page 388.

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 the "SCCP: Setting a Mailbox Selection Policy for Cisco Unity Express or a PBX Voice-Mail Number" section on page 383 or the "SCCP: Setting Mailbox Selection Policy for Cisco Unity" section on page 384.

RFC 2833 DTMF MTP Passthrough

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 the "Enabling DTMF Integration Using RFC 2833" section on page 390.

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 the"SCCP: Configuring a Voice Mailbox Pilot Number" section on page 381 or "SIP: Configuring a Directory Number for MWI" section on page 397.

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 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 informations, see the "SCCP: Configuring a Phone for MWI Outcall" section on page 395.

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 the "Enabling SIP MWI Prefix Specification" section on page 401.

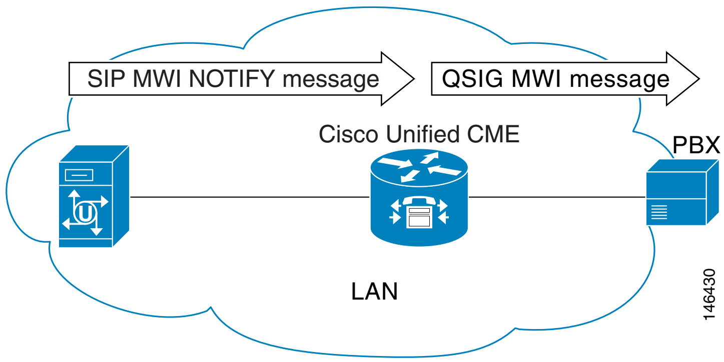
SIP MWI - QSIG Translation

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 17, 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.

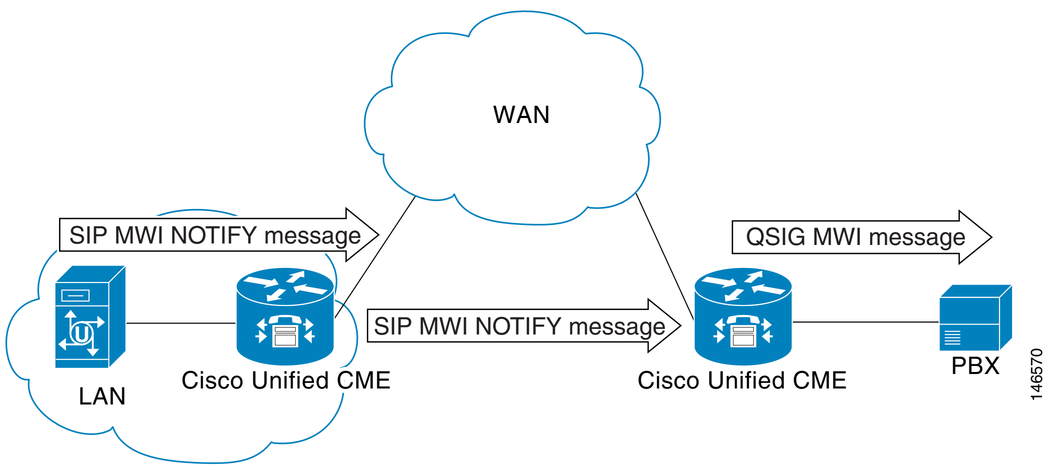
Figure 17 SIP MWI to ISDN QSIG When Voice Mail and Cisco Router are On the Same LAN



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 18, 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 18 SIP MWI to ISDN QSIG When PBX is Connected to a Remote Cisco Router



How to Configure Voice-Mail Integration

This section contains the following tasks:

- SCCP: Configuring a Voice Mailbox Pilot Number, page 381 (required)
- SCCP: Configuring a Mailbox Selection Policy, page 383 (optional)
- SIP: Configuring a Voice Mailbox Pilot Number, page 386 (required)
- Enabling DTMF Integration, page 388 (required)
- SCCP: Configuring a Phone for MWI Outcall, page 395 (optional)
- SIP: Enabling MWI at the System-Level, page 396 (required)
- SIP: Configuring a Directory Number for MWI, page 397 (required)

- Enabling SIP MWI Prefix Specification, page 401 (optional)
- Verifying Voice-Mail Integration, page 401 (optional)

SCCP: Configuring a Voice Mailbox Pilot Number

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.

Prerequisites

- Voicemail phone number must be a valid number; directory number and number for voicemail phone number must be configured. For configuration information, see "Configuring Phones to Make Basic Calls" on page 165.

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.
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.

	Command or Action	Purpose
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 the "SCCP: Configuring a Mailbox Selection Policy" section on page 383.
- To set up DTMF integration patterns for connecting to analog voice-mail applications, see the "Enabling DTMF Integration for Analog Voice-Mail Applications" section on page 388.
- 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 the "Enabling DTMF Integration Using RFC 2833" section on page 390.
- To connect to a Cisco Unity Express system, configure a nonstandard SIP NOTIFY format. See the "Enabling DTMF Integration Using SIP NOTIFY" section on page 393.

SCCP: Configuring a Mailbox Selection Policy

Perform *one* of the following tasks, depending on which voice-mail application is used:

- SCCP: Setting a Mailbox Selection Policy for Cisco Unity Express or a PBX Voice-Mail Number, page 383
- SCCP: Setting Mailbox Selection Policy for Cisco Unity, page 384

SCCP: Setting 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.

Prerequisites

Cisco Unified CME 4.0 or a later version.

Restrictions

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.

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` or `Router(config)# dial-peer voice 35 pots`	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.
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 the "Enabling DTMF Integration Using SIP NOTIFY" section on page 393.

SCCP: Setting 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.

Prerequisites

- Cisco Unified CME 4.0 or a later version.
- Director number to be configured is associated with a voice mailbox.

Restrictions

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **mailbox-selection last-redirect-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	**`exit`** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.

	Command or Action	Purpose
Step 4	**ephone-dn** **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 the "Enabling DTMF Integration Using RFC 2833" section on page 390.

SIP: Configuring a Voice Mailbox Pilot Number

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.

Prerequisites

- Directory number and number for voicemail phone number must be configured. For configuration information, see "Configuring Phones to Make Basic Calls" on page 165.

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*
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.
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.

	Command or Action	Purpose
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 the "Enabling DTMF Integration for Analog Voice-Mail Applications" section on page 388.
- 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 the "Enabling DTMF Integration Using RFC 2833" section on page 390.
- To connect to a Cisco Unity Express system, configure a nonstandard SIP NOTIFY format, see the "Enabling DTMF Integration Using SIP NOTIFY" section on page 393.

Enabling DTMF Integration

Perform *one* of the following tasks, depending on which DTMF-relay method is required:

- Enabling DTMF Integration for Analog Voice-Mail Applications, page 388—To set up DTMF integration patterns for connecting to analog voice-mail applications.
- Enabling DTMF Integration Using RFC 2833, page 390—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.
- Enabling DTMF Integration Using SIP NOTIFY, page 393—To configure a SIP dial peer to point to Cisco Unity Express.

Enabling 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • 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).

	Command or Action	Purpose
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.
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 the "SCCP: Configuring a Phone for MWI Outcall" section on page 395.

Enabling 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.

Prerequisites

- Configure the **codec** or **voice-class codec** command for transcoding between G.711 and G.729. See "Configuring Phones to Make Basic Calls" on page 165.

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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> 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.

	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	**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	**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 the "SCCP: Configuring a Phone for MWI Outcall" section on page 395.

Enabling DTMF Integration Using SIP NOTIFY

To configure a SIP dial peer to point to Cisco Unity Express and enable SIP dual-tone multifrequency (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.
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	**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 the "SCCP: Configuring a Phone for MWI Outcall" section on page 395.

SCCP: Configuring a 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.

Prerequisites

- Directory number and number for MWI line must be configured. For configuration information, see "Configuring Phones to Make Basic Calls" on page 165.

Restrictions

- 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.

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.
Step 3	`ephone` *phone-tag* **Example:** `Router(config)# ephone 36`	Enters ephone configuration mode.

	Command or Action	Purpose
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 "SCCP: Enabling Ephone-dn Templates" on page 930.
Step 9	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to privileged EXEC mode.

SIP: Enabling MWI at the System-Level

To enable a message waiting indicator (MWI) at a system-level, perform the following steps.

Prerequisites

- 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.

SIP: Configuring a Directory Number for MWI

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.

- SIP: Defining Pilot Call Back Number for MWI Outcall, page 398
- SIP: Configuring a Directory Number for MWI NOTIFY, page 399

SIP: Defining 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.

Prerequisites

- Cisco CME 3.4 or a later version.
- Directory number and number for receiving MWI must be configured. For configuration information, see "Configuring Phones to Make Basic Calls" on page 165.

Restrictions

- 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.

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.
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.

	Command or Action	Purpose
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.

SIP: Configuring 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.

Prerequisites

- 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 "Enabling H.450.7 and QSIG Supplementary Services at a System-Level" on page 553 or "Enabling H.450.7 and QSIG Supplementary Services on a Dial Peer" section on page 554.
- Directory number and number for receiving MWI must be configured. For configuration information, see "Configuring Phones to Make Basic Calls" on page 165.

Restrictions

- 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.

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.
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.

Enabling 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.

Prerequisites

- Cisco Unified CME 4.0 or a later version.
- Directory number for receiving MWI Unsolicited NOTIFY must be configured. For information, see "SIP: Configuring a Directory Number for MWI NOTIFY" section on page 399.

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.
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.

Verifying 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

This section contains the following examples:

Enabling DTMF Integration for Legacy Voice-Mail Applications: Example

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 *
```

Enabling Mailbox Selection Policy for SCCP Phones: Example

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
```

Configuring a Voice Mailbox: Example

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
```

Enabling DTMF Integration Using RFC 2833: Example

The following example shows the configuration for a DTMF Relay:

```
dial-peer voice 1 voip
 destination-pattern 4…
 session target ipv4:10.8.17.42
 session protocol sipv2
 dtmf-relay sip-notify rtp-nte
```

Enabling DTMF Integration Using SIP Notify: Example

The following example shows the configuration for a DTMF Relay:

```
dial-peer voice 1 voip
 destination-pattern 4…
 session target ipv4:10.5.49.80
 session protocol sipv2
 dtmf-relay sip-notify
 b2bua
```

Configuring a SCCP Phone Line for MWI: Example

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
```

Enabling SIP MWI Prefix Specification: Example

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
```

Configuring SIP Directory Number for MWI Outcall: Example

The following example shows an MWI callback pilot number:

```
voice register dn
 number 9000….
 mwi
```

Configuring a SIP Directory Number for MWI Unsolicited Notify: Example

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
```

Configuring a SIP Directory Number for MWI Subscribe/NOTIFY: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Voice-Mail Integration

Table 22 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 22 lists the 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.

Table 22 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.
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.
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.

Configuring Security

Last Updated: July 30, 2007

This chapter describes the phone authentication support in Cisco Unified Communications Manager Express (Cisco Unified CME) and the Media Encryption (SRTP) on Cisco Unified CME feature which provide 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.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Security" section on page 477.

Contents

Prerequisites for Security

Phone Authentication

- Cisco Unified CME phone authentication requires the Cisco IOS feature set Advanced Enterprise Services (adventerprisek9) or Advanced IP Services (advipservicesk9) on supported platforms.
- Set the system clock using one of these methods:
  - Configure Network Time Protocol (NTP).
  - Manually set the software clock using the **clock set** command.

  Both methods are explained in the "Performing Basic System Management" chapter of the *Cisco IOS Network Management Configuration Guide* for your Cisco IOS release.

Media Encryption

- Cisco Unity 4.2 or later version
- Cisco Unified CME 4.2 or a later version
- Cisco IOS Release 12.4(11)XW or a later release on the Cisco VG224 Analog Phone Gateway

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 conference 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 does not support SIP trunks; only H.323 trunks are supported.

Table 23 lists supported gateways, network modules, and codecs for Media Encryption (SRTP) on Cisco Unified CME.

Table 23 Supported Gateways, Network Modules, and IP Phones for Media Encryption (SRTP) on Cisco Unified CME

Supported Gateways	Supported Network Modules	Supported SCCP Endpoints
• Cisco 2801 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3725 • Cisco 3745 • Cisco 3825 • Cisco 3845	• AIM-VOICE-30 • AIM-ATM-VOICE-30 • NM-HDA-4FXS • NM-HDV • NM-HDV2 • NM-HDV2-1T1/E1 • NM-HDV2-2T1/E1 • NM-HD-1V • NM-HD-2V • NM-HD-2VE • PVDM2	• Cisco IP Phone 7931 • Cisco IP Phone 7940 • Cisco IP Phone 7941 • Cisco IP Phone 7941GE • Cisco IP Phone 7960 • Cisco IP Phone 7961 • Cisco IP Phone 7961GE • Cisco IP Phone 7970 • Cisco IP Phone 7971 • Cisco IP Phone 7911 • Cisco IP Phone 7921 • Cisco VG224 Analog Phone Gateway

Information About Security

To enable security, you should understand the following concepts:

Phone Authentication

Media Encryption

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 upon the following processes:

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 secure transport-layer-session (TLS) 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 secured data network. Every entity (a person or a device) participating in the secured 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 secured 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.

For more information about PKI, see the "Implementing and Managing a PKI" section of the *Cisco IOS Security Configuration Guide* for your Cisco IOS release.

Phone Authentication Components

A variety of components work together to ensure secure communications in a Cisco Unified CME system. Table 24 describes the Cisco Unified CME phone authentication components.

Table 24 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.

Table 24 Cisco Unified CME Phone Authentication Components (continued)

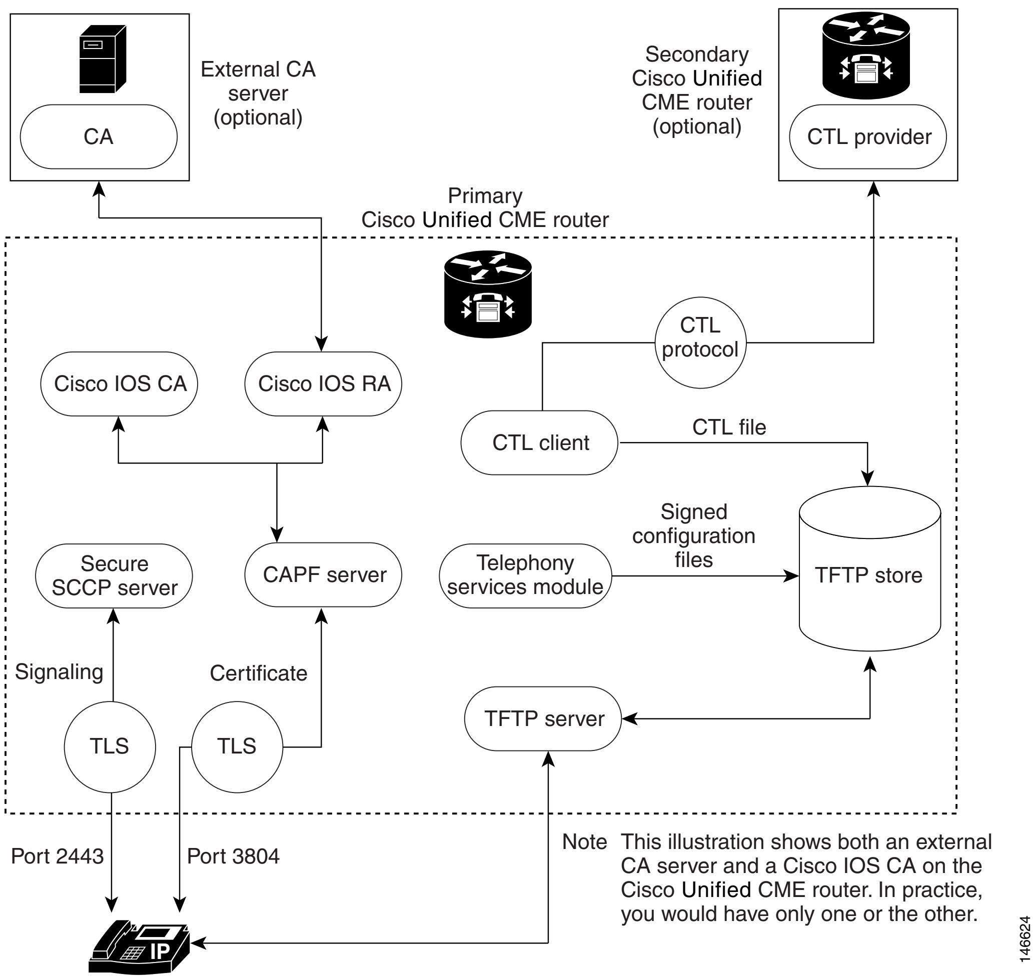
Component	Definition
RSA key pair	RSA is a public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. An RSA key pair consists of a public key and a private key. The public key is included in a certificate so that peers can use it to encrypt data that is sent to the router. 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.
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 system administrator security token (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.

Table 24 Cisco Unified CME Phone Authentication Components (continued)

Component	Definition
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.
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 locally significant certificates 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 19 shows the components in a Cisco Unified CME phone authentication environment.

Figure 19 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 the "Configuring the CTL Client" section on page 441 and the "Configuring the CTL Provider" section on page 446.

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 in order 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.

For more information on certificate enrollment, see the "Configuring Cut-and-Paste Certificate Enrollment" section of the "Configuring Certificate Enrollment for a PKI" chapter in the *Cisco IOS Security Configuration Guide* for your Cisco IOS release.

To manually import the MIC root certificate, see the "Manually Importing MIC Root Certificate" section on page 434.

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:

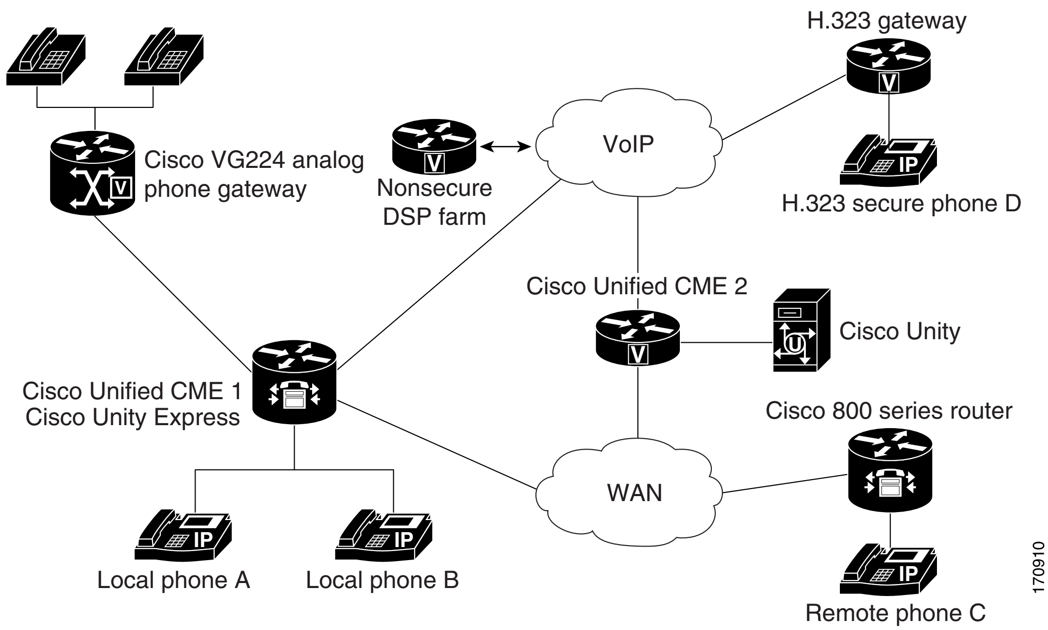
- SRTP capable Cisco Unified CME networks with secure interoperability
- Secure Cisco IP phone calls
- Secure Cisco VG224 Analog Phone Gateway endpoints
- Secure supplementary services

We implement these features 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. We use H.450 messages 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 20 shows the components of a secure Cisco Unified CME system.

Figure 20 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 to gateways.

The Media Encryption (SRTP) on Cisco Unified CME feature supports the following features:

- Secure voice calls using SRTP for 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 0 to 2 second noise interval when the call is joined to the conference.

- Secure calls in a nonH.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.

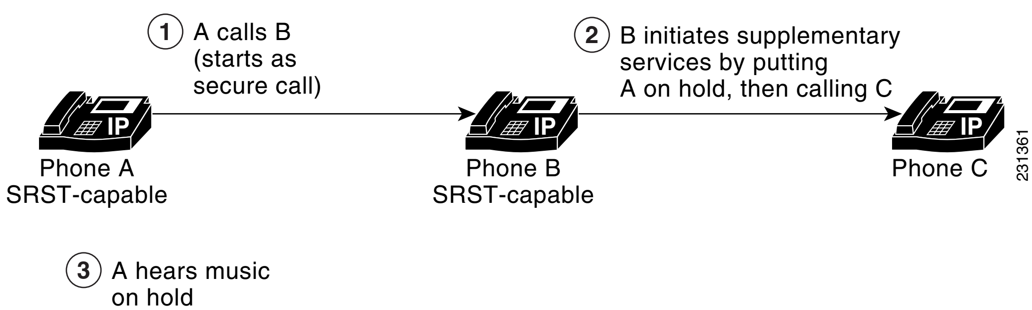
Secure Supplementary Services

The Media Encryption (SRTP) feature supports secure supplementary services in both H.450 and nonH.450 Cisco Unified CME networks. A secure Cisco Unified CME network should be either H.450 or nonH.450, not a hybrid.

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 21, 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.

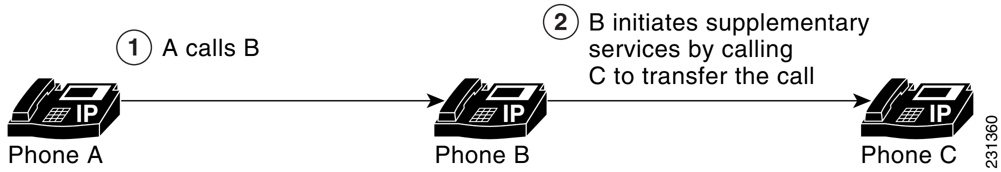
Figure 21 Music on Hold in an H.450 Environment



Secure Cisco Unified CME in a NonH.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 22 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 22 Transfer in a NonH.45 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 that 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 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 which 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 in order 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.

Secure Cisco Unified CME with Cisco Unity Express

Note 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), was 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."

How to Configure Security

This section contains the following tasks:

Phone Authentication

Media Encryption

Configuring the Cisco IOS Certification Authority

To configure a root certificate server, also called a certification authority (CA), on a Cisco IOS router, perform the following steps. The router can be the Cisco Unified CME router or an external router.

Setting up a Cisco IOS CA is a standard PKI task. The basic steps are included here for ease of use. For more information, see the "Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment" section in "Part 5: Implementing and Managing a PKI" in the *Cisco IOS Security Configuration Guide* for your Cisco IOS release.

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 certificate server and enters certificate-server configuration mode. • *label*—Name for CA certificate server.

	Command or Action	Purpose
Step 5	**database level** {**minimal** | **names** | **complete**} **Example:** `Router(config-cs-server)# database level complete`	(Optional) Controls the type of data stored in the certificate enrollment database. • **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. • **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 by using the **database url** command.
Step 6	**database url** *root-url* **Example:** `Router(config-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	**lifetime certificate** *time* **Example:** `Router(config-cs-server) lifetime certificate 888`	(Optional) Specifies the lifetime, in days, of certificates issued by this CA server. • *time*—Number of days until a certificate expires. Range is 1 to 1825. Default is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate. **Note** If you want to use this command is used, use it before the server is enabled with the **no shutdown** command.
Step 8	**issuer-name CN=***name* **Example:** `Router(config-cs-server)# issuer-name CN=sanjose1`	(Optional) Specifies a distinguished name (DN) as the certification-authority (CA) issuer name for the certificate server. If the issuer name is not configured, CN = CA label.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config-cs-server)# exit`	Exits certificate-server configuration mode.
Step 10	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint sanjose1`	(Optional) Declares a trustpoint and enters ca-trustpoint configuration mode. • *label*—Name for the trustpoint. • A trustpoint for the CA is automatically generated by the router when the CA is started. If you must use a specific RSA key for the CA, you can create your own trustpoint by using the same label used in the **crypto pki server** command in Step 13. If the router sees a configured trustpoint with the same label as that of the "crypto pki server," it uses this trustpoint and does not automatically create a 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 on an external router.
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 CA certificate server (root certificate server). • *ca-url*—URL of the router on which the root 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 for CA certificate server.
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. **Tip** 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.

	Command or Action	Purpose
Step 15	**no shutdown** **Example:** `Router(config-cs-server)# no shutdown`	(Optional) Enables the CA. **Note** You should use this command only after you have completely configured the CA.
Step 16	**end** **Example:** `Router(config-cs-server)# end`	Returns to privileged EXEC mode.

Verifying the Cisco IOS Certification Authority

Step 1 Use the **show crypto pki server** command to display the status of the certificate server.

Step 2 Use the **show running-config** command to display the running configuration, including the certificate-server configuration.

The following example defines a CA named authority1 running locally on the Cisco Unified CME router:

```
ip http server

crypto pki server authority1
 database level complete
 database url nvram:

crypto pki trustpoint authority1
 enrollment url http://ca-server.company.com

crypto pki server authority1
 no grant auto
 no shutdown
```

Configuring the Registration Authority

This task is required if the CA is a third-party CA or if the CA is on a Cisco IOS router external to the Cisco Unified CME router. In these cases, the CAPF server requires an RA to issue certificates to phones.

The 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 Cisco IOS certificate server 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. The certificate-server label that you use here is also used in the **crypto pki server** command in Step 9. **Note** This name is also specified in the **cert-enroll-trustpoint** command when you set up the CA proxy as described in the "Configuring the CAPF Server" section on page 448.
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 certificate server (root certificate server). • *ca-url*—URL of the router on which the root CA has been installed.

	Command or Action	Purpose
Step 5	**revocation-check** *method1* [*method2* [*method3*]] **Example:** `Router(config-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. 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. **Note** 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. The certificate-server label must have the same name as the trustpoint that was created in Step 3.
Step 10	**mode ra** **Example:** `Router(config-cs-server)# mode ra`	Places the PKI server into certificate-server mode for the RA.

	Command or Action	Purpose
Step 11	**lifetime certificate** *time* **Example:** `Router(config-cs-server)# lifetime certificate 1800`	(Optional) Specifies the lifetime, in days, of a certificate. • *time*—Number of days until the certificate expires. Range is 1 to 1825. Default is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate. **Note** If this command is used, it 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. **Note** Use this command only during enrollment when testing and building simple networks. As a security best practice, disable this functionality after configuration using the **no grant auto** command so that certificates are not continually granted.
Step 13	**no shutdown** **Example:** `Router(config-cs-server)# no shutdown`	(Optional) Enables the certificate server. You are prompted to provide input regarding acceptance of the CA certificate, the router certificate, the challenge password, and a password for protecting the private key. **Note** 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.

Verifying the Registration Authority

Step 1 Use the **show crypto pki server** command to display the status of the certificate server.

Step 2 Use the **show crypto pki certificates** command to display certificate information.

Step 3 Use the **show running-config** command to display the running configuration.

Authenticating Certificates for Server Functions

The Cisco Unified CME router needs certificates for the following server functions:

- Secure SCCP server (Cisco Unified CME)—Requires a certificate for TLS sessions with phones.
- TFTP server credentials—Requires a key pair and certificate for signing configuration files.
- CAPF server—Requires a certificate for TLS sessions with phones.
- Security tokens—Required for signing the CTL file. We recommend creating two certificates, one for primary use and the other for backup.

To obtain a certificate for each of these functions, perform the following steps for each server function.

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 Cisco Unified CME certificate server should use and enters ca-trustpoint configuration mode. • *trustpoint-label*—Label for the trustpoint.
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 certificate server (root certificate server). • *url*—URL of the router on which the root CA is installed.

	Command or Action	Purpose
Step 5	**revocation-check** *method1* [*method2* [*method3*]] **Example:** `Router(config-ca-trustpoint)# revocation-check none`	(Optional) Checks the revocation status of a certificate. • *method*—Method used by the router to check the revocation status of the certificate. 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. – **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*—(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. **Note** Multiple trustpoints can share the same key.
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 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 9	**crypto pki enroll** trustpoint-label **Example:** `Router(config)# crypto pki enroll capf`	Enrolls with the CA and obtains the certificate for this trustpoint. • *trustpoint-label*—Trustpoint label.
Step 10	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Verifying Certificates for Server Functions

Step 1 Use the **show crypto pki certificates** command to display information about the certificates.

Step 2 Use the **show running-config** command to display the running configuration.

Manually Importing 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.

Prerequisites

One of the following situations must be true before you perform this task:

- You choose to use MIC as the method for phone authentication during CAPF certificate operation
- You plan to establish the TLS session for SCCP signaling using the phone's MIC instead of an LSC

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **revocation-check** *method1*
5. **enrollment terminal**
6. **exit**
7. **crypto pki authenticate** *name*
8. Open the MIC root file and copy the certificate.
9. When prompted, paste the certificate, press Enter, and type **quit**.
10. Enter **y** to accept the certificate.
11. **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*—CA trustpoint name.
Step 4	**`revocation-check`** *`method1`* **Example:** `Router(ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate. • *method1*—The method used by the router to check the revocation status of the certificate. For this task, the only available method is **none**. The keyword **none** is required for this task and means that a 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.
Step 7	**`crypto pki authenticate`** *`name`* **Example:** `Router(config)# crypto pki authenticate sanjose1`	Authenticates the CA (by getting the certificate from the CA). • *name*—Name of the CA.
Step 8	Open the MIC root file and copy the certificate.	The MIC root file is a file with name a*.0, located in the directory C:\Program Files\Cisco\Certificates Copy to a buffer or temporary location all of the contents that appear between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".
Step 9	When prompted, paste the certificate, press Enter, and type **quit**.	Paste the text from the a*.0 file, press Enter after pasting the certificate, and type **quit** on a line by itself.

	Command or Action	Purpose
Step 10	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.
Step 11	`exit` **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Configuring Telephony-Service Security Parameters

To enable telephony-service security parameters, 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** {**secure** | **non-secure**}
10. **exit**
11. **ephone** *phone-tag*
12. **device-security-mode** {**authenticated** | **none** | **encrypted**}
13. **codec** {**g711ulaw** | **g729r8** [**dspfarm-assist**]}
14. **capf-auth-str** *digit-string*
15. **cert-oper** {**delete** | **fetch** | **upgrade**} **auth-mode** {**auth-string** | **LSC** | **MIC** | **null-string**}
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	**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`	Specifies the name of the PKI trustpoint that has the valid certificate to be used for TLS handshakes with IP phones on TCP port 2443. • *label*—Name of a configured PKI trustpoint with a valid certificate.
Step 5	**tftp-server-credentials trustpoint** *label* **Example:** `Router(config-telephony)# tftp-server-credentials trustpoint cme-tftp`	Specifies the name of the PKI trustpoint to be used to sign the phone configuration files. This can be the CAPF-server trustpoint that was used in the previous step or any trustpoint with a valid certificate. • *label*—Name of a configured PKI 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 all security-capable phones in the system. • **authenticated**—SCCP signaling between a device and Cisco Unified CME takes place through the secure TLS connection on TCP port 2443. • **none**—SCCP signaling is not secure. This is the default. • **encrypted**—SCCP signaling between a device and Cisco Unified CME takes place through the secure TLS connection on TCP port 2443, and the media uses Secure Real-Time Transport Protocol (SRTP). Use the **encrypted** keyword to enable Secure Cisco Unified CME functionality. **Note** You can override the setting you make in this command for individual ephones by using the **device-security-mode** command in ephone configuration mode.

	Command or Action	Purpose
Step 7	**cnf-file perphone** **Example:** `Router(config-telephony)# cnf-file perphone`	Specifies the generation of a separate configuration file for each individual phone. Separate configuration files for each endpoint are required for security.
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. To serve an already signed file on the TFTP server, use this command without the **sign** and **create** keywords. • *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. **Note** The first time that you use this command for each file, use the **create** keyword in addition to the **sign** keyword. The **create** keyword is not maintained in the running configuration to prevent signed files from being recreated during every reload.
Step 9	**server-security-mode** {**secure** | **non-secure**} **Example:** `Router(config-telephony)# server-security-mode secure`	(Optional) Changes the security mode of the server. • **secure**—Secure mode. • **non-secure**—Nonsecure mode. **Note** 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. **Note** This command must be followed by the **regenerate** command in CTL-client configuration mode.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits telephony-service configuration mode.
Step 11	**ephone** *phone-tag* **Example:** `Router(config)# ephone 24`	Enters ephone configuration mode. • *phone-tag*—Identifier of the ephone to be configured.

	Command or Action	Purpose
Step 12	**device-security-mode** {**authenticated** | **none** | **encrypted**} **Example:** `Router(config-ephone)# device-security-mode authenticated`	(Optional) Sets the security mode for SCCP signaling for an ephone communicating with the Cisco Unified CME router. • **authenticated**—SCCP signaling between a device and Cisco Unified CME takes place 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 takes place through the secure TLS connection on TCP port 2443, and the media uses Secure Real-Time Transport Protocol (SRTP). Use the **encrypted** keyword to enable Secure Cisco Unified CME functionality. **Note** You can set this value globally using the **device-security-mode** command in telephony-service configuration mode. A per-phone setting in ephone configuration mode overrides the global setting for that phone.
Step 13	**codec** {**g711ulaw** | **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**—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. The **dspfarm-assist** keyword is ignored if the SCCP endpoint type is ATA, VG224, or VG248. **Note** The **dspfarm-assist** keyword is required for secure transcoding with Cisco Unified CME to work.
Step 14	**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. Use the show **capf-server auth-string** command to display configured strings. For instructions on how to enter the string from the phone, see the "Entering the Authentication String on the Phone" section on page 452. • *digit-string*—String of digits that the phone user must dial for CAPF authentication. The string can be from 4 to 10 digits in length. **Note** You can set this value globally using this command or per ephone using the **auth-string** command in CAPF-server configuration mode.

	Command or Action	Purpose
Step 15	**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 this ephone. • **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**—Phone user enters a special authentication string at the phone. The string is set with the **capf-auth-str** command and is provided to the phone user by the system administrator. See the "Entering the Authentication String on the Phone" section on page 452. • **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. If this option is chosen, the MIC's issuer certificate must be imported into a PKI trustpoint. See the "Manually Importing MIC Root Certificate" section on page 434. • **null-string**—No authentication. **Note** You can initiate certificate operations globally using the **cert-oper** command in CAPF-server configuration mode. You can set authentication mode globally using the **auth-mode** command in CAPF-server configuration mode.
Step 16	**reset** **Example:** `Router(config-ephone)# reset`	Performs a complete reboot of the phone.
Step 17	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verifying 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.

```
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 capf-server auth-string**

Use this command to display authentication strings for phones.

```
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
```

Step 3 **show running-config**

Use this command to display the running configuration to verify telephony and per-phone security configuration.

```
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
.
.
.
```

Configuring the CTL Client

The tasks to configure the CTL client differ slightly depending on whether the CTL client is running on the same router as Cisco Unified CME. Choose the appropriate procedure based on your network:

- Configuring the CTL Client on a Cisco Unified CME Router, page 442
- Configuring the CTL Client on a Router Other Than a Cisco Unified CME Router, page 444

Configuring the CTL Client on a Cisco Unified CME Router

The credentials of various functions are included in the CTL file, which is created and hosted on the TFTP server. To configure a CTL client on a Cisco Unified CME router, perform the following steps.

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** *trustpoint-label*
5. **sast2 trustpoint** *trustpoint-label*
6. **server** {**capf** | **cme** | **cme-tftp** | **tftp**} *ip-address* **trustpoint** *trustpoint-label*
7. **server cme** *ip-address* **username** *string* **password 0** *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*—SAST1 trustpoint name. **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 5	**sast2 trustpoint** *label* **Example:** `Router(config-ctl-client)# sast2 trustpoint`	Configures credentials for the secondary SAST. • *label*—SAST2 trustpoint name. **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 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. **Note** Repeat this command with the appropriate keyword for each function that is running locally on the Cisco Unified CME router. • **capf**—CAPF server. • **cme**—Cisco Unified CME router. • **cme-tftp**—Combined Cisco Unified CME router and TFTP server. • **tftp**—TFTP server. • *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 entity.
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 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. • *password-string*—Administrative password of the CTL provider running on the remote Cisco Unified CME router.

	Command or Action	Purpose
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.

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. See the "Configuring the CTL Provider" section on page 446.

Configuring the CTL Client on a Router Other Than a Cisco Unified CME Router

To configure a CTL client on an external 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** *trustpoint-label*
5. **sast2 trustpoint** *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.

	Command or Action	Purpose
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*—SAST1 trustpoint name. **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*—SAST2 trustpoint name. **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.

	Command or Action	Purpose
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.

What to do Next

You must configure a CTL provider on each Cisco Unified CME router. See the "Configuring the CTL Provider" section on page 446.

Verifying the CTL Client

Step 1 Use the **show ctl-client** command to display the CTL client configuration.

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
```

Configuring the CTL Provider

If you have more than one Cisco Unified CME router in your network, perform the following steps to configure a CTL provider on each Cisco Unified CME router on which the CTL client is not running.

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.
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*—Router 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. You should use 2444.
Step 5	**trustpoint** *trustpoint-label* **Example:** `Router(config-credentials)# trustpoint ctlpv`	Configures the trustpoint to be used for TLS sessions with the CTL client. • *trustpoint-label*—CTL provider trustpoint label.
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. You must use this command before you enable the CTL provider. • *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.

Verifying the CTL Provider

Step 1 **show credentials**

Use this command to display credentials settings.

```
Router# show credentials

Credentials IP: 172.19.245.1
Credentials PORT: 2444
Trustpoint: ctlpv
```

Configuring 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. **port** *tcp-port*
8. **auth-mode** {**auth-string** | **LSC** | **MIC** | **none** | **null-string**}
9. **auth-string** {**delete** | **generate**} {**all** | *ephone-tag*} [*auth-string*]
10. **phone-key-size** {**512** | **1024** | **2048**}
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** **Example:** `Router> enable`	Enables privileged EXEC mode. • 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 of the trustpoint whose certificate is to be used for TLS connection between the CAPF server and the phone. • *label*—Trustpoint name.
Step 5	**cert-enroll-trustpoint** *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). • *trustpoint-label*—PKI trustpoint label for the CA or RA. • **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. • *ip-address*—IP address of the CAPF server.
Step 7	**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.

	Command or Action	Purpose
Step 8	**auth-mode** {**auth-string** | **LSC** | **MIC** | **none** | **null-string**} **Example:** `Router(config-capf-server)# auth-mode auth-string`	Specifies the type of authentication to use during 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. See the "Manually Importing MIC Root Certificate" section on page 434. • **none**—No certificate upgrade is initiated. This is the default. • **null-string**—No authentication.
Step 9	**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 all the secure ephones or for specified secure ephones. Use this command if the **auth-string** keyword is specified in the **auth-mode** command. Strings become part of the ephone configuration. Use the **show capf-server auth-string** command to view authentication strings. • **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*—String of digits that the phone user must dial for CAPF authentication. The string can be 4 to 10 digits. If this value is not specified, a random string is generated for each phone. For instructions on how to enter the string from the phone, see the "Entering the Authentication String on the Phone" section on page 452. **Note** You can also define an authentication string for an individual ephone using the **capf-auth-str** command.
Step 10	**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.

	Command or Action	Purpose
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, in minutes. • *minutes*—Number of minutes before the generation process times out. Range is 1 to 120. Default is 30.
Step 13	**cert-oper** {**delete all** | **fetch all** | **upgrade all**} **Example:** `Router(config-capf-server)# cert-oper upgrade all`	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. **Note** You can use the **cert-oper** command in ephone configuration mode for certificate operations on individual ephones. See the "Configuring Telephony-Service Security Parameters" section on page 436.
Step 14	**end** **Example:** `Router(config-capf-server)# end`	Returns to privileged EXEC mode.

What to Do Next

If you select the authentication-string method of authentication in the **auth-mode** command, you must also enter an authentication string on each phone that is receiving an updated LSC. For instructions on this task, see the "Entering the Authentication String on the Phone" section on page 452.

Verifying the CAPF Server

Step 1 **show capf-server summary**

Use this 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
```

Step 2 **show capf-server auth-string**

Use this command to display configured strings (PINs) that users enter at the phone to establish CAPF authentication:

```
Router# show capf-server auth-string

Authentication Strings for configured Ephones
Mac-Addr        Auth-String
--------        -----------
000CCE3A817C    7012
001121116BDD    922
000D299D50DF    9182
000ED7B10DAC    3114
000F90485077    3328
0013C352E7F1    0678
```

Entering 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 specify the authentication string method of authentication.

If an authentication string is defined using the **auth-string** command in CAPF-server configuration mode or the **capf-auth-str** command in ephone configuration mode, the authentication string must be communicated to the phone user so that it can be entered on the phone before the LSC is installed.

The phone user can perform the following procedure to install the certificate. The authentication string applies for one-time use only.

Note You can list authentication strings for phones by using the **show capf-server auth-string** command.

Prerequisites

- The CAPF certificate exists in the CTL file.
- A signed image exists on the phone; see the Cisco Unified IP phone administration documentation that supports your phone model.
- The device has registered.
- The device security mode is nonsecure.

DETAILED STEPS

Step 1 Press the Settings button.

On the Cisco Unified IP Phone 7921, use the down arrow key 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 soft key.

Step 4 Scroll down the Security Configuration menu. Highlight LSC and press the Update soft key.

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 soft key.

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" displays 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 the Stop option at any time.

Verifying the Authentication String on the Phone

Step 1 Verify that the certificate was installed on the phone by choosing Settings > Model Information and viewing the LSC setting, which indicates Installed or Not Installed.

Configuring Secure Calls Between Cisco Unified CMEs Across an H.323 Trunk

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.

Prerequisites

To make secure H.323 calls, telephony-service security parameters must be configured. See the "Configuring Telephony-Service Security Parameters" section on page 436.

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`	Enables security policies. • The **srtp** command enables secure calls using SRTP for media encryption and authentication and disables fallback. • The **fallback** keyword enables call fallback to nonsecure (RTP) mode, allowing the user to make calls that are not secure. • SRTP-to-RTP fallback must be configured for supplementary services such as ringback tone and MOH to function. Without SRTP-to-RTP fallback configured, MOH causes secure calls to be dropped. **Note** This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. If fallback is not configured it will drop all calls that are not secure so only secure phones can call you. This step configures fallback globally. To configure fallback for individual dial peers, see the "Configuring Cisco Unified CME SRTP Fallback for H.323 Dial Peers" section on page 455. Skip this step if you are going to configure fallback on individual dial peers.
Step 6	**h323** **Example:** `Router(conf-voi-serv)# h323`	Enters H.323 voice-service configuration mode.

	Command or Action	Purpose
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.

Configuring 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.

Note SRTP-to-RTP fallback must be configured for supplementary services such as ringback tone and MOH to function. Without SRTP-to-RTP fallback configured, MOH causes secure calls to be dropped.

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.

	Command or Action	Purpose
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.
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 security and causes the dial peer to fall back to RTP mode. • The **srtp** command enables secure calls. • The **fallback** keyword enables fallback to nonsecure mode (RTP) on an individual dial peer. The **no** form of this command disables fallback and disables SRTP. **Note** This dial-peer configuration command takes precedence over the globally configured **srtp** command enabled in voice service voip configuration mode shown in the "Configuring Secure Calls Between Cisco Unified CMEs Across an H.323 Trunk" section on page 453.
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.

Configuring Cisco Unity for Secure Cisco Unified CME Operation

This section contains the following tasks:

- Configuring Integration Between Cisco Unified CME and Cisco Unity, page 457
- Importing the Cisco Unity Root Certificate to Cisco Unified CME, page 458
- Configuring Cisco Unity Ports for Secure Registration, page 459
- Verifying that Cisco Unity are Registering Securely, page 459

Configuring 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 already open, on the Cisco Unity server, on the Windows Start menu, click **Programs** > **Cisco Unity** > **Manage Integrations**. The UTIM window appears.

Step 2 In the left pane, double-click **Cisco Unity Server**. The existing integrations appear.

Step 3 Click the **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 the Non-secure setting, click **Save** and skip the remaining steps in this procedure.

If you clicked the Authenticated or the Encrypted settings, the Security tab and the Add TFTP Server dialog box appear. In the Add TFTP Server dialog box, in the IP Address or Host Name field, 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 file name 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.

Importing 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.
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) 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 5	`enrollment terminal` **Example:** `Router(ca-trustpoint)# enrollment terminal`	Specifies manual cut-and-paste certificate enrollment.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits CA-trustpoint configuration mode.
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 if prompted. • *trustpoint-label*—Trustpoint label. **Note** The *trustpoint-label* must be the same as the *name* in step 3.
Step 8	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.

Configuring 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 In the Device Security Mode field, choose **Encrypted** from the drop-down list box.

Step 3 Click **Update**.

Verifying 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.

show sccp connection: Example

In the following example, the secure value of the stype 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
```

Configuration Examples for Security

This section contains the following examples:

Phone Authentication

Media Encryption

Cisco IOS CA Server: Example

```
!
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 ...
```

Enabling a Registration Authority: Example

The following example sets up an RA and trustpoint named ra12:

```
Router(config)# crypto pki trustpoint ra12
Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com
Router(config-ca-trustpoint)# revocation-check none
Router(config-ca-trustpoint)# rsakeypair exampleCAkeys 1024 1024
Router(config-ca-trustpoint)# exit
Router(config)# crypto pki server ra12
Router(config-cs-server)# mode ra
Router(config-cs-server)# lifetime certificate 1800
Router(config-cs-server)# no grant auto
Router(config-cs-server)# no shutdown
Router(config-cs-server)# exit
```

The following example sets up a trustpoint named sast2 that periodically generates a CRL instead of having it generated manually. Third-party CAs may require this functionality.

```
Router(config)# crypto pki trustpoint sast2
Router(config-ca-trustpoint)# enrollment url http://NTP-ab11:80
Router(config-ca-trustpoint)# serial-number
Router(config-ca-trustpoint)# revocation-check crl
Router(config-ca-trustpoint)# rsakeypair sast2
```

Manually Importing MIC Root Certificate on the Cisco Unified CME Router: Example

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 were granted. The five certificates include the three certificates just entered and 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
```

Obtaining a Certificate for Cisco Unified CME Server Functions: Example

The following example establishes a trustpoint for the CAPF server called capf.

```
Router(config)# crypto pki trustpoint capf
Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com
Router(config-ca-trustpoint)# revocation-check none
Router(config-ca-trustpoint)# rsakeypair capf 1024 1024
Router(config-ca-trustpoint)# exit
Router(config)# crypto pki authenticate capf
Router(config)# crypto pki enroll capf
```

Telephony-Service Security Parameters: Example

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
```

CTL Client Running on Cisco Unified CME Router: Example

```
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
!
```

Secure Cisco Unified CME: Example

```
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 10000
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 3084
 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
 no multicast-moh
 device-security-mode encrypted
 mac-address 0012.4302.A7CC
 type 7970
 button  1:1
!
!
!
ephone  2
 no multicast-moh
 device-security-mode encrypted
 mac-address 0017.94CA.9CCD
 type 7960
 button  1:2
!
!
!
ephone  3
 no multicast-moh
 device-security-mode encrypted
 mac-address 0017.94CA.9833
 type 7960
 button  1:3
!
!
!
ephone  4
 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
```

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). For more information, see the following documents:

- "Part 5: Implementing and Managing a PKI" in the *Cisco IOS Security Configuration Guide* for your Cisco IOS release.
- *Cisco IOS Security Command Reference* for your Cisco IOS release.

Cisco VG224 Analog Phone Gateway

- To configure secure endpoints on the Cisco VG224 Analog Phone Gateway, see *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways*.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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	• "Implementing and Managing a PKI" section in the *Cisco IOS Security Configuration Guide*. • *Cisco IOS Voice Configuration Library* • *Cisco IOS Software Releases 12.4T Configuration Guides*
Phone documentation for Cisco Unified CME	• Quick Reference Cards and User Guides
Cisco VG224 Analog Phone Gateway	• *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways* • *Cisco VG224 Voice Gateway Software Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Security

Table 25 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 25 lists the 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.

Table 25 Feature Information for Security

Feature Name	Cisco Unified CME Version	Feature Information
Media Encryption (SRTP) on Cisco Unified CME	4.2	Media encryption on Cisco Unified CME was introduced.
Phone Authentication	4.0	Phone authentication for Cisco Unified CME phones was introduced.

Configuring Automatic Line Selection

Last Updated: March 26, 2007

This chapter describes automatic line selection features in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Automatic Line Selection" section on page 484.

Contents

Information About Automatic Line Selection

To enable automatic line selection, you should understand the following concept:

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.

How to Configure Automatic Line Selection

This section contains the following tasks:

- Enabling Automatic Line Selection, page 480 (required)
- Verifying Automatic Line Selection, page 482 (optional)

Enabling Automatic Line Selection

To enable automatic line selection for answering incoming calls or making outgoing calls, perform the following steps:

Restrictions

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** **Example:** `Router> 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 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.

Verifying 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.

```
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.

```
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

This section contains the following example:

Automatic Line Selection: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Automatic Line Selection

Table 26 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 26 lists the 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.

Table 26 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.

Configuring Call Blocking

Last Updated: July 26, 2007

This chapter describes Call Blocking features in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Call Blocking" section on page 501.

Contents

Information About Call Blocking

To configure call blocking features, you should understand the following concepts:

- Call Blocking Based on Date and Time (After-Hours Toll Bar), page 486
- Call Blocking Override, page 486
- Class of Restriction, page 487

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. Up to 32 patterns of digits can be specified. Call blocking is supported on IP phones only and not on analog foreign exchange station (FXS) phones.

When a user attempts to place a call to digits that match a pattern that 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.

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 phones is expanded to SIP endpoints. Call blocking to prevent unauthorized use of Cisco Unified IP phones is implemented by matching a pattern of specified digits during a particular time of the day and day of the week or date.You can specify up to 32 patterns of digits for blocking.

Prior to Cisco CME 3.4, call blocking is supported on IP phones and on analog phones connected to SCCP-controlled analog telephone adaptors (Cisco ATA) or SCCP-controlled foreign exchange station (FXS) ports. This feature supports incoming SIP and analog FXS calls. 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.

The Cisco Unified CME session application accesses the current after-hours configuration and applies it to calls originated by SIP phones that are registered to the Cisco Unified CME router. The after-hours commands are the same as for SCCP phones in Cisco Unified CME.

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

For configuration information, see the "Configuring Call Blocking Based on Date and Time" section on page 492.

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 the following sections:

- "Configuring Call Blocking Exemption for a Dial Peer" section on page 493.
- "SCCP: Configuring Call Blocking Exemption for an Individual Phone" section on page 494.
- "SIP: Configuring Call Blocking Exemption for an Individual Phone or Directory Number" section on page 495.

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 configuration information, see the "SCCP: Applying Class of Restriction to a Directory Number" section on page 488.

How to Configure Call Blocking

This section contains the following tasks:

SCCP: Applying Class of Restriction to a Directory Number

To apply a class of restriction to a directory number, perform the following steps.

Prerequisites

- COR lists must be created in dial peers. For information, see the "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 "SCCP: Creating Directory Numbers" on page 177.

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** **Example:** `Router> 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 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.

SIP: Applying Class of Restriction to Directory Number

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.

Prerequisites

- Cisco unified CME 3.4 or a later version.
- COR lists must be created in dial peers. For information, see the "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 "SIP: Creating Directory Numbers" on page 181.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-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	**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	**cor** {**incoming** | **outgoing**} *cor-list-name* {*cor-list-number starting-number* [**-** *ending-number*] | **default**} **Example:** `Router(config-register-pool)# cor incoming call91 1 91011`	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.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Verifying 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.

```
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.

```
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.

```
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.
```

Configuring Call Blocking Based on Date and Time

To define dial patterns and time periods during which calls to those dial patterns are blocked, perform the following steps.

Restrictions

- Before Cisco CME 3.3, call blocking is not supported on analog phones connected to Cisco ATAs or FXS ports in H.323 mode.
- Before Cisco CME 3.4, call blocking is not supported on SIP IP phones connected directly in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **after-hours block pattern** *tag pattern* [**7-24**]
5. **after-hours day** *day start-time stop-time*
6. **after-hours date** *month date start-time stop-time*
7. **login** [**timeout** [*minutes*]] [**clear** *time*]
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	**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.

	Command or Action	Purpose
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.
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.
Step 7	**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. • Only for IP phones running SCCP. • *minutes*—(Optional) Range: 1 to 1440. Default: 60. Before Cisco Unified CME 4.1, the minimum value for this argument was 5 minutes.
Step 8	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

Configuring 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.
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.

SCCP: Configuring Call Blocking Exemption for an Individual Phone

To exempt all directory numbers associated with an individual SCCP phone from the call blocking configuration, follow the steps in this section.

Restrictions

Call blocking override is supported only on phones that support soft-key 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—N*umber from four to eight digits in length.
Step 6	**`end`** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

SIP: Configuring Call Blocking Exemption for an Individual 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.

Restrictions

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` or `Router(config)# voice register dn 1`	Enters voice register pool configuration mode to set parameters for specified SIP phone. or 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-dn)# end` or `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

Verifying Call Blocking Based on Date and Time

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.

```
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.

```
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.

Configuration Examples for Call Blocking

This section contains the following examples:

- Call Blocking: Example, page 497
- Class of Restriction: Example, page 498

Call Blocking: Example

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
```

Class of Restriction: Example

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
!
dial-peer voice 2 pots
 corlist outgoing call-local
 destination-pattern 9[2-9]......
 port 2/0/0
!
dial-peer voice 3 pots
 corlist outgoing call-911
 destination-pattern 9911
 port 2/0/0
!
```

```
ephone-dn 1
 corlist incoming user1
 corlist outgoing user1
!
ephone-dn 2
 corlist incoming user2
 corlist outgoing user2
```

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 "Resetting and Restarting Phones" on page 277.

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 "Customizing Soft Keys" on page 875.

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 "Creating Templates" on page 927.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Call Blocking

Table 27 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 27 lists the 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.

Table 27 Feature Information for Call Blocking

Feature Name	Cisco Unified CME Version	Feature Information
Call Blocking	3.4	Added support for call blocking on SIP IP phones connected directly in Cisco Unified CME.
	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	3.4	Added support for COR on SIP IP Phones connected directly in Cisco Unified CME.
	2.0	Class of restriction was introduced.

Configuring Call Park

Last Updated: March 26, 2007

This chapter describes the call park feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Call Park" section on page 516.

Contents

Information About Call Park

To enable call park, you should understand the following concepts:

Basic Call Park

Call park allows a phone user to place a call on hold at a special ephone-dn that is used as a temporary parking spot from which the call can be retrieved by anyone on the system. In contrast, a call that is placed on hold using the Hold button or Hold soft key can be retrieved only from the extension that placed the call on hold. The special ephone-dn at which a call is parked is known as a *call-park slot*. A call-park slot is a floating extension, or ephone-dn that is not bound to a physical phone, to which calls are sent to be held.

After at least one call-park slot has been defined and the Cisco Unified CME phones have been restarted, phone users are able to park calls using the Park soft key. Users who attempt to park a call at a busy slot hear a busy tone.

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, a feature that is available in Cisco CME 3.2 and later versions; otherwise, callers hear a tone on hold.

A phone user who has parked a call can retrieve the call using the PickUp soft key and an asterisk (*). Phone users other than the one who parked the call can retrieve the call by pressing the PickUp soft key and the extension number of the call-park slot, which is available on their phone displays.

Directed call park allows calls to be transferred to a call-park-slot extension number using the Transfer key; a transfer to a call-park slot is always a blind transfer. Calls can also be forwarded from phones to call-park slot numbers. For 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 and later versions, a direct call to a call-park slot is interpreted as an attempt to pick up a call that is parked there; if no call is parked in the slot, the caller hears a busy tone.

The ability to directly dial a park slot to retrieve a call is useful in the following scenario. An attendant connected to a remote Cisco Unified CME system can perform a directed call park (transfer-to-park) into a park slot on the local Cisco Unified CME router by simply transferring the call to the telephone number associated with the local Cisco Unified CME park slot. The remote attendant can then inform local phone users of the existence of the parked call by dialing (across VoIP) into a paging number on the local Cisco Unified CME system, or the parked call may simply be visible to one or more local users whose phones are configured to monitor the park-slot. Then, when a local IP phone user directly dials the extension number of the park slot, the system assumes that the user is requesting retrieval (pickup) of the call in the park slot. If there is no call in the park slot, the Cisco Unified CME system returns a busy tone to the local user.

A caller who is parked in a park slot hears the music-on-hold (MOH) audio stream if the call uses a G.711 codec or if it uses G.729 with transcoding, a feature that is available in Cisco CME 3.2 and later versions; otherwise, callers hear a tone on hold.

Each call-park slot occupies one ephone-dn. During configuration, any number of ephone-dns can be designated as call-park slots using the **park-slot** command, provided the total number of park slots and normal extensions does not exceed the maximum number of ephone-dns that was defined with the **max-dn** command. After an administrator defines at least one call-park slot and restarts phones, the Park soft key is displayed on all IP phones that are able to display soft keys.

Each call-park slot can hold one call at a time, so the number of simultaneous calls that can be parked is equal to the number of slots that have been created in the Cisco Unified CME system. In Cisco CME 3.2.1 and later releases, call-park slots can also be monitored. If a call-park slot is assigned 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 to which to transfer a parked call if the recall or transfer target is in use. *In use* is defined as either 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 23. 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.

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.

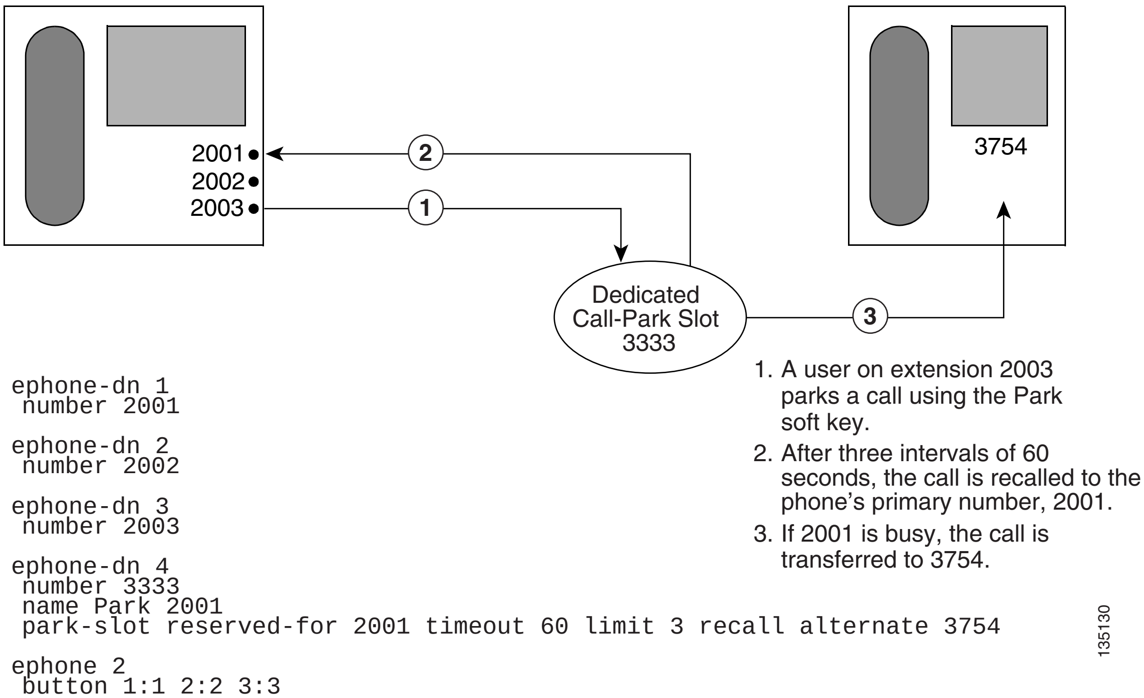
If no dedicated park slot is found anywhere in the Cisco Unified CME system for an ephone-dn that is attempting to park a call, the system uses the standard call-park procedure; that is, the system searches for a preferred park slot (one with an ephone-dn number that matches the last two digits of the ephone-dn attempting to park the call) and if none is found, uses any available call-park slot.

Figure 23 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 23 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 23 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 23 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 "Customizing Soft Keys" on page 875.)

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.

How to Configure Call Park

This section contains the following tasks:

- Enabling Call Park, page 508
- Verifying Call Park, page 512
- Troubleshooting Call Park, page 513

Enabling Call Park

To enable call-park slots, optional call-park blocking, or call-park redirect, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
5. **park-slot** [**reserved-for** *extension-number*] [**timeout** *seconds* **limit** *count*] [**notify** *extension-number* [**only**]] [**recall**] [**transfer** *extension-number*] [**alternate** *extension-number*] [**retry** *seconds* **limit** *count*]
6. **exit**
7. **ephone** *phone-tag*
8. **transfer-park blocked**
9. **exit**
10. **telephony-service**
11. **call-park system redirect**
12. **restart all**
13. **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-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. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. • **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	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 2345`	Configures a valid extension number for this ephone-dn instance. • *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. Unless you specify one of the optional keywords (**both** or **primary**) after the **no-reg** keyword, only the secondary number is not registered.

	Command or Action	Purpose
Step 5	**park-slot** [**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 reserved-for 2458 timeout 60 limit 3 recall alternate 3754`	Creates a floating extension (ephone-dn) at which calls can be temporarily held (parked). • **reserved-for** *extension-number*—(Optional) Indicates that this slot is a private park slot for the phone with the specified extension number as its primary line. All lines on that phone can use this park slot. • **timeout** *seconds*—(Optional) Sets the call-park reminder timeout interval, in seconds. Range is 0 to 65535. When the interval expires, the call-park reminder sends a 1-second ring and displays a message on the LCD panel of the Cisco Unified IP phone that parked the call and that of any extension that may be specified with the **notify** keyword. Default is that the reminder ring is sent only to the phone that parked the call. • **limit** *count*—(Optional, applies to **timeout** keyword) Sets a limit for the number of time-out intervals for a parked call. For example, a limit of 3 sends 2 reminder rings (interval 1, ring 1, interval 2, ring 2, interval 3). A call parked at this slot is disconnected after the limit has been reached unless another action has been specified. Range is 1 to 65535. • **notify** *extension-number*—(Optional) Sends a reminder ring to the specified extension in addition to the reminder ring that is sent to the phone that parked the call. • **only**—(Optional) Sends a reminder ring only to the extension specified with the notify keyword and does not send a reminder ring to the phone that parked the call. This option allows all reminder rings for parked calls to be sent to a receptionist's phone or an attendant's phone, for example. • **recall**—(Optional) Returns the call to the phone that parked it after the timeout limits expire. • **transfer** *extension-number*—(Optional) Returns the call to the specified number after timeout limits expire. • **alternate** *extension-number*—(Optional) Returns the call to the specified second target number if the recall or transfer target phone is in use on any of its extensions (ringing or in conversation). • **retry** *seconds*—(Optional) Sets the delay before another attempt to recall or transfer a parked call, in seconds. Range is 0 to 65535. Number of attempts is set by the **limit** keyword. • **limit** *count*—(Optional, applies to **retry** keyword) Sets a limit for the number of retries. When a limit is set, a call parked at this slot is disconnected after the limit has been reached. Range is 1 to 65535.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 7	**ephone** *phone-tag* **Example:** `Router(config)# ephone 25`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 8	**transfer-park blocked** **Example:** `Router(config-ephone)# transfer-park blocked`	(Optional) Prevents extensions on this ephone from transferring calls to call-park slots. **Note** This command prevents the use of the Transfer soft key and slot number to transfer calls to park slots. It does not prevent use of the Park soft key.
Step 9	**exit** **Example:** `Router(config-telephony)# exit`	Exits ephone configuration mode.
Step 10	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 11	**call-park system redirect** **Example:** `Router(config)# call-park system redirect`	Specifies that within the call-park feature, H.323 and SIP calls will use H.450 or the SIP Refer method of call forwarding or transfer to park calls and to pick up calls from park. The **no** form of the command returns to the default behavior, which is to use hairpin call forwarding or transfer to park calls and pick up calls from park.
Step 12	**restart all** **Example:** `Router(config)# restart all`	Performs a fast reboot of all phones associated with this Cisco Unified CME router. Does not contact the DHCP server. **Note** The first time that call-park slots are defined, IP phones must be rebooted before the Park soft key is displayed on phones. This command is not required after subsequent call-park slot definitions.
Step 13	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.

Verifying 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.

```
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.

```
Router# show telephony-service ephone-dn

ephone-dn  26
 number 8136 secondary 136
 park-slot reserved-for 136 timeout 10 limit 1 recall
```

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 the *Cisco Unified CME Command Reference*.

Configuration Examples for Call Park

This section contains the following examples:

Basic Call Park: Example

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
```

Phone Blocked From Using Call Park: Example

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
```

Call-Park Redirect: Example

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
```

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 "Customizing Soft Keys" on page 875.

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 "Customizing Soft Keys" on page 875.

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 "Creating Templates" on page 927.

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 "Customizing Soft Keys" on page 875.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Call Park

Table 28 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 28 lists the 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.

Table 28 Feature Information for Call Park

Feature Name	Cisco Unified CME Version	Feature Information
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.

Configuring Call Transfer and Forwarding

Last Updated: May 23, 2007

This chapter describes call transfer and forwarding features in Cisco Unified Communications Manager Express (Cisco Unified CME) to enable interworking with various network requirements.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Call Transfer and Forwarding" section on page 579.

Contents

Information About Call Transfer and Forwarding

To configure transfer and forwarding features, you should understand the following concepts:

Call Forwarding

Call forwarding 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 the "SCCP: Enabling Call Forwarding for a Directory Number" section on page 541.

Selective Call Forwarding

You can apply call forwarding 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 the "SCCP: Enabling Call Forwarding for a Directory Number" section on page 541.

B2BUA Call Forwarding 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 the "SIP: Configuring SIP-to-SIP Phone Call Forwarding" section on page 564.

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 the "SIP: Configuring Call-Forwarding-All Soft Key URI" section on page 566.

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 interoperate 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 systemwide 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.

Consultative Transfer With Direct Station Select

Direct Station Select (DSS) is a feature that allows a multibutton 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 "Configuring Conferencing" on page 665.

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.

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 24 on page 522 shows A calling B. Figure 25 on page 522 shows B consulting with C and putting A on hold. Figure 26 on page 523 shows that B has connected A and C, and Figure 27 on page 523 shows A and C directly connected, with B no longer involved in the call.

Figure 24 Call Transfer Using H.450.2: A Calls B

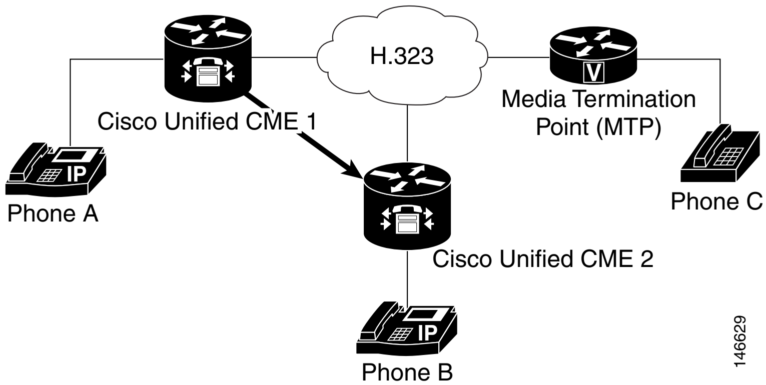


Figure 25 Call Transfer Using H.450.2: B Consults with C

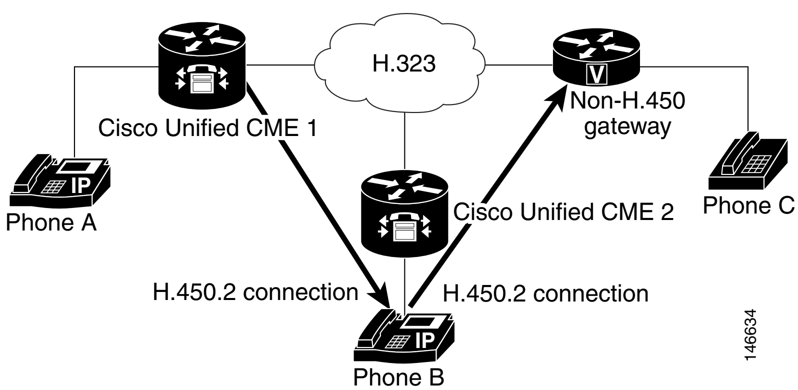


Figure 26 Call Transfer Using H.450.2: B Transfers A to C

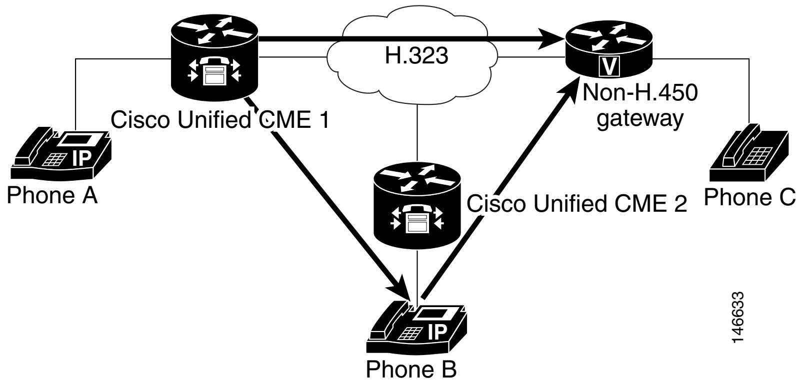
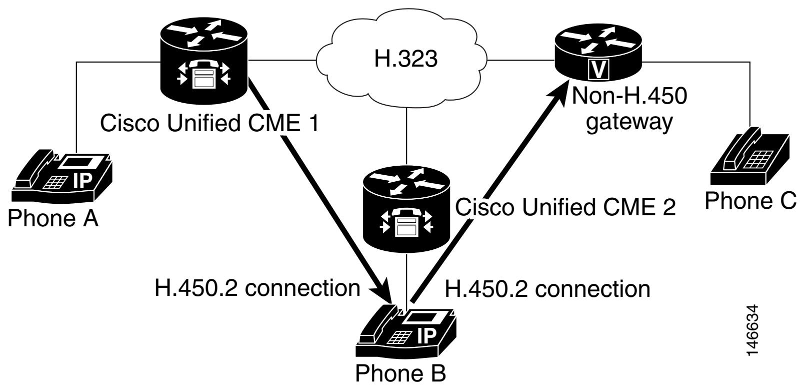


Figure 27 Call Transfer Using H.450.2: A and C Are Connected



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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.

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 29 summarizes transfer method recommendations for all Cisco Unified CME versions.

Table 29 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.
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 http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp. For configuration information, see the *Cisco IOS Telephony Services Version 2.1* guide.
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 the "Enabling H.450.12 Capabilities" section on page 547.

    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 the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549. 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"Enabling H.323-to-H.323 Connection Capabilities" section on page 549. 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. For information about transcoding, see "Configuring Transcoding Resources" on page 323.

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 28 on page 526 shows a call that is made from A to B. Figure 29 on page 527 shows that B has forwarded all calls to C. Figure 30 on page 527 shows that A and C are connected by an H.323 hairpin.

Figure 28 Hairpin with H.323: A Calls B

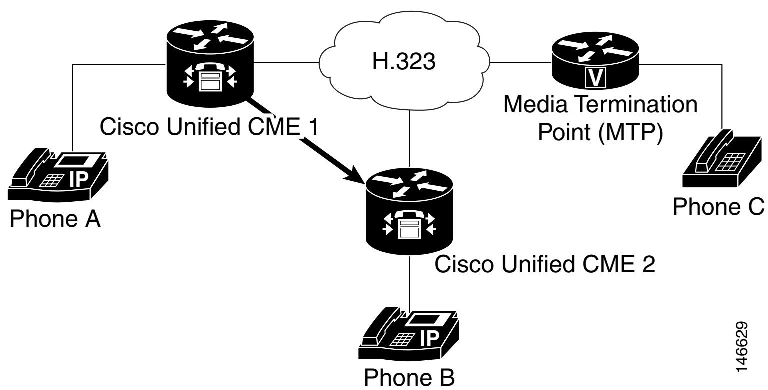


Figure 29 Hairpin with H.323: Call is Forwarded to C

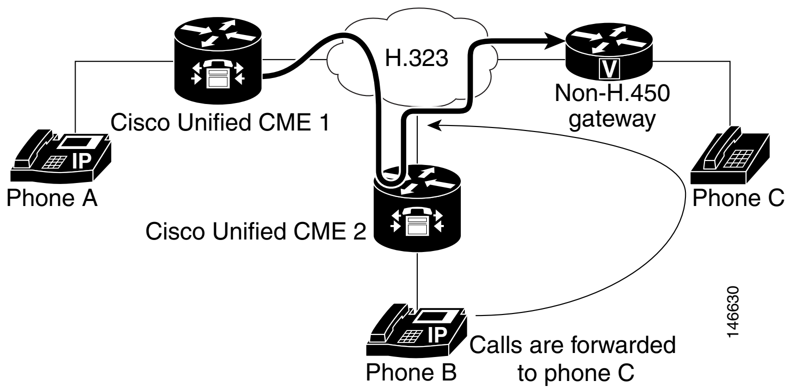
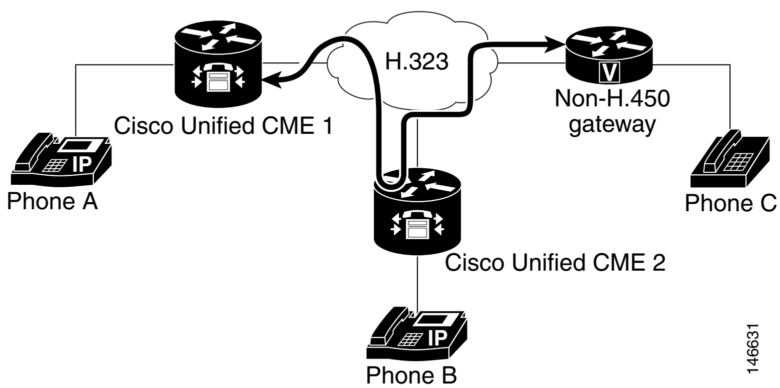


Figure 30 Hairpin with H.323: A is Connected to C via B



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 the "Enabling H.450.12 Capabilities" section on page 547.
- 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 the "Forwarding Calls Using Local Hairpin Routing" section on page 551.

Support for VoIP-to-VoIP connections is disabled by default and can be enabled globally. For configuration information, see the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.

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.

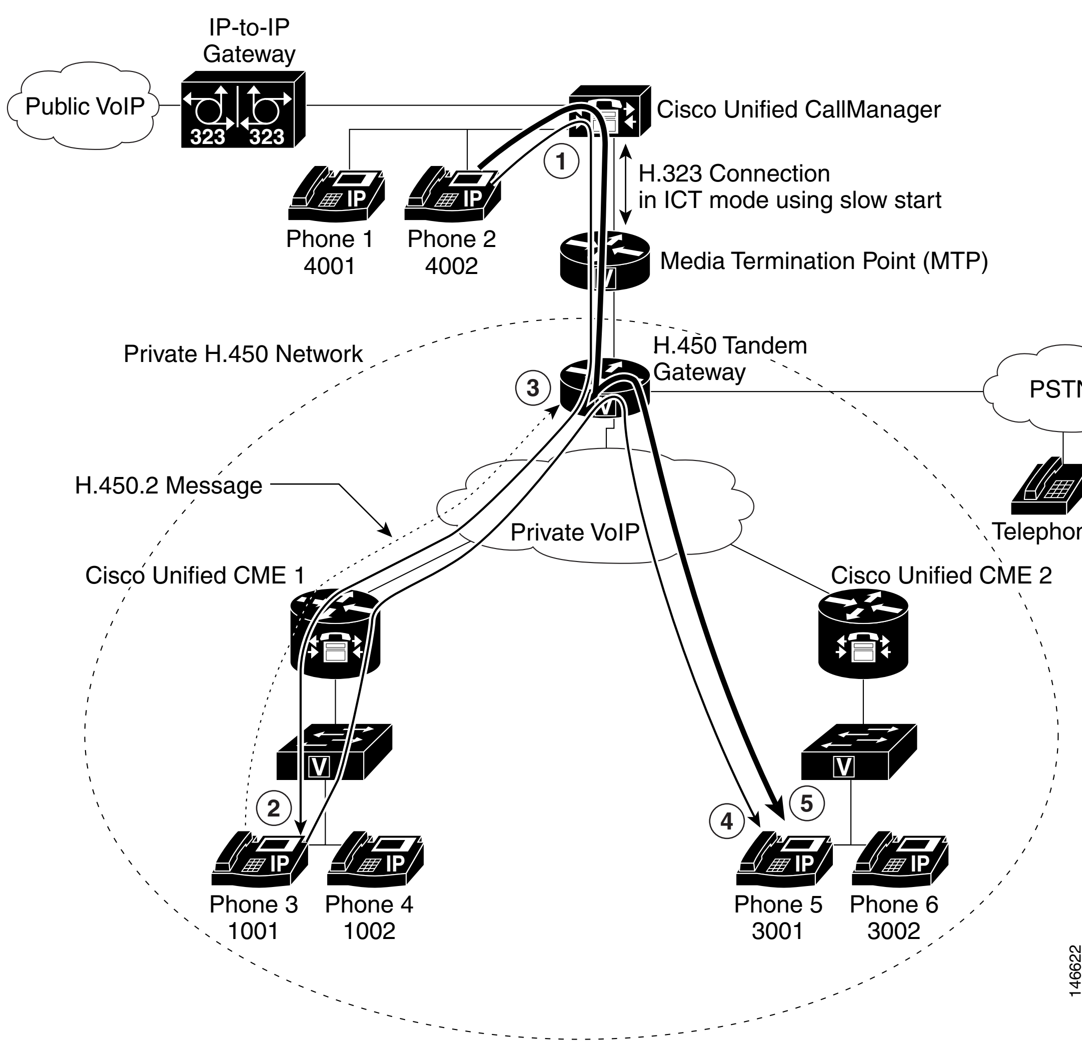
For Cisco CME 3.1 and earlier, the only type of VoIP-to-VoIP connection supported by Cisco Unified CME is H.323-to-H.323. For Cisco CME 3.2 and later versions, H.323-to-SIP connections are allowed only for Cisco Unified CME systems running Cisco Unity Express.

Figure 31 on page 529 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 31 on page 529, 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 31 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 the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.

Use dial peers to set up an H.450 tandem gateway. See the "Dial Peers" section on page 530.

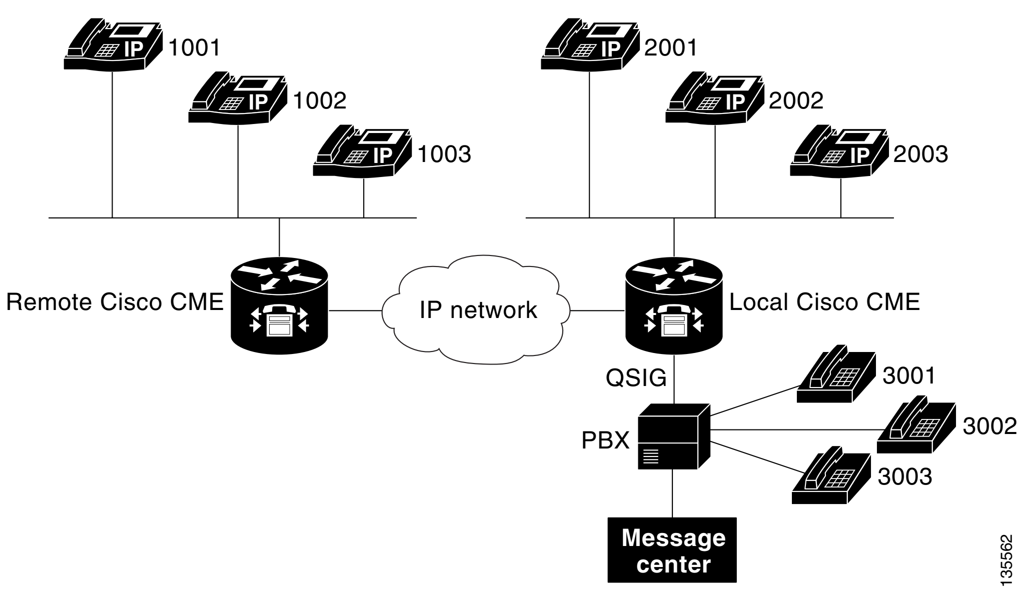
Dial Peers

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. For information about configuring dial peers, see the *Dial Peer Configuration on Voice Gateway Routers* guide.

QSIG Supplementary Services

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 32 illustrates a topology for a Cisco Unified CME system with some phones under the control of a PBX.

Figure 32 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 the "Enabling H.450.7 and QSIG Supplementary Services at a System-Level" section on page 553 and "Enabling H.450.7 and QSIG Supplementary Services on a Dial Peer" section on page 554.

For more information about configuring Cisco Unified CME to integrate with voice-mail systems, see "Integrating Voice Mail" on page 375.

Disabling SIP Supplementary Services for Call Forward and Call Transfer

If a destination gateway does not support supplementary services, you can disable REFER messages for call transfers and redirect responses for call forwarding from being sent by Cisco Unified CME or Cisco Unified SRST.

Disabling supplementary services is supported if all endpoints use SCCP or all endpoints use SIP. It is not supported for a mix of SCCP and SIP endpoints.

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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.
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 the "Enabling H.450.12 Capabilities" section on page 547.
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 the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.
4. Setting up dial peers to manage call legs within the network. See *Dial Peer Configuration on Voice Gateway Routers*.

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:

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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.
2. 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 the "Enabling H.450.12 Capabilities" section on page 547.
3. 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 the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.
4. Setting up dial peers to manage call legs within the network. See *Dial Peer Configuration on Voice Gateway Routers*.

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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.
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 the "Enabling H.450.12 Capabilities" section on page 547.
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 the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.
4. Setting up dial peers to manage call legs within the network. See *Dial Peer Configuration on Voice Gateway Routers*.

Note If your network contains a Cisco Unified Communications Manager, also see the instructions in the "Enabling Interworking with Cisco Unified Communications Manager" section on page 558.

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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.
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 the "Enabling H.450.12 Capabilities" section on page 547.
3. Setting up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route all transferred and forwarded calls. See the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.
4. Setting up dial peers to manage call legs within the network. See *Dial Peer Configuration on Voice Gateway Routers*.

Note If your network contains a Cisco Unified Communications Manager, also see the instructions in the "Enabling Interworking with Cisco Unified Communications Manager" section on page 558.

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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.

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 the "Enabling H.450.12 Capabilities" section on page 547.
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. See the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.
4. Setting up specific parameters for Cisco Unified Communications Manager. See the instructions in the "Enabling Interworking with Cisco Unified Communications Manager" section on page 558.
5. Setting up dial peers to manage call legs within the network. See *Dial Peer Configuration on Voice Gateway Routers*.

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. See the configuration instructions in the "Configuring Call Transfer" chapter of the *Cisco CallManager Express 3.0 System Administrator Guide*.
- Use a loopback-dn mechanism. See "Configuring Loopback Call Routing" on page 809.
- 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).

In addition to the special considerations above, configuration of the Cisco CME 3.1 or later router 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 the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.
2. Leaving H.450.12 capability in its default disabled state. For more information, see the "Enabling H.450.12 Capabilities" section on page 547.
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. See the "Enabling H.323-to-H.323 Connection Capabilities" section on page 549.

4. Setting up specific parameters for Cisco Unified Communications Manager. See the instructions in the "Enabling Interworking with Cisco Unified Communications Manager" section on page 558.
5. Setting up dial peers to manage call legs within the network. See *Dial Peer Configuration on Voice Gateway Routers*.

How to Configure Call Transfer and Forwarding

This section contains the following procedures:

SCCP

SIP B2BUA

Enabling Call Transfer and Forwarding 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.

Prerequisites

Cisco CME 3.0 or a later version, or Cisco ITS V2.1.

Restrictions

- Call transfers are handled differently depending on the Cisco Unified CME version. See Table 29 on page 524 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.

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. **exit**
8. **voice service voip**
9. **supplementary-service h450.2**
10. **supplementary-service h450.3**
11. **exit**
12. **dial-peer voice** *tag* **voip**
13. **supplementary-service h450.2**
14. **supplementary-service h450.3**
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	**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. • 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.) • **blind**—Calls are transferred without consultation with a single phone line using the Cisco proprietary method. This is the default in Cisco CME versions earlier than 4.0. • **full-blind**—Calls are transferred without consultation using H.450.2 standard methods. • **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. • **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.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 5</td><td><code>transfer-pattern transfer-pattern [blind]</code>

Example:
<code>Router(config-telephony)# transfer-pattern .T</code></td><td>Allows transfer of telephone calls by Cisco Unified IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones.
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.
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. For more information, see “Configuring Dialing Plans” on page 287.</td></tr>
<tr><td>Step 6</td><td><code>call-forward pattern pattern</code>

Example:
<code>Router(config-telephony)# call-forward pattern .T</code></td><td>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, as described in the “Configuring Call Forwarding” chapter in the Cisco IOS Telephony Services Version 2.1 guide.
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.
Note For forwards 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. For more information, see “Configuring Dialing Plans” on page 287.</td></tr>
<tr><td>Step 7</td><td><code>exit</code>

Example:
<code>Router(config-telephony)# exit</code></td><td>Exits telephony-service configuration mode.</td></tr>
<tr><td>Step 8</td><td><code>voice service voip</code>

Example:
<code>Router(config)# voice service voip</code></td><td>(Optional) Enters voice-service configuration mode to establish global call transfer and forwarding parameters.</td></tr>
</table>

	Command or Action	Purpose
Step 9	**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 10	**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 11	**exit** **Example:** `Router(conf-voi-serv)# exit`	(Optional) Exits voice-service configuration mode.
Step 12	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	(Optional) Enters dial-peer configuration mode.
Step 13	**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.

	Command or Action	Purpose
Step 14	**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. • 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. • 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 15	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

SCCP: Enabling 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. For more information, see the "Voice Translation Rules and Profiles" section in "Configuring Dialing Plans" on page 287.

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.
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.

	Command or Action	Purpose
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 "Configuring Call-Coverage Features" on page 581.
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.

SCCP: Enabling 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.

Prerequisites

Call transfer must be enabled globally. See the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **transfer-mode** {**blind** | **consult**}
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`* `[`**`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	**`end`** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

SCCP: Configuring Call Transfer Options for Phones

To specify a maximum number of digits for transfer destinations or block transfers to external destinations by individual phones, perform the following steps.

Restrictions

- 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 sequence number that identifies this template during configuration tasks. Range is 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.

	Command or Action	Purpose
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.
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`	Returns to privileged EXEC mode.

SCCP: Verifying Call Transfer

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.

```
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.

```
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.

Enabling 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.

Restrictions

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.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	(Optional) Enters dial-peer configuration mode.

	Command or Action	Purpose
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.

Enabling H.323-to-H.323 Connection Capabilities

VoIP-to-VoIP connections 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 the "Enabling H.450.12 Capabilities" section on page 547.
- Explicitly disable H.450.2 and H.450.3 capabilities globally or on the routes that your transfers and forwards take. See the "Enabling Call Transfer and Forwarding at System-Level" section on page 537.

Restrictions

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

Forwarding 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.
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	**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. **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`	Returns to privileged EXEC mode.

Enabling H.450.7 and QSIG Supplementary Services at a System-Level

To enable H.4350.7 capabilities and QSIG supplementary services on all dial peers, perform the following steps.

Prerequisites

Cisco Unified CME 4.0 or a later version.

Restrictions

- 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.

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.

	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	**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`	Returns to privileged EXEC mode.

Enabling 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.

Prerequisites

Cisco Unified CME 4.0 or a later version.

Restrictions

- 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.

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.
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.

	Command or Action	Purpose
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** `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`	Returns to privileged EXEC mode.

Disabling 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.

Prerequisites

Cisco Unified CME 4.1 or a later version.

Restrictions

Disabling supplementary services is supported only when all endpoints are SCCP or all endpoints are SIP. It does not support a mix of SCCP and SIP endpoints.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **voice service voip**
   or
   dial-peer voice *tag* **voip**
4. **no supplementary-service sip** {**moved-temporarily** | **refer**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	`enable` **Example:** `Router> 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` or `dial-peer voice` *tag* `voip` **Example:** `Router(config)# voice service voip` or `Router(config)# dial-peer voice 99 voip`	Enters voice-service configuration mode to set global parameters for VoIP features. or Enters dial peer configuration mode to set parameters for a specific dial peer.
Step 4	`no supplementary-service sip {moved-temporarily | refer}` **Example:** `Router(conf-voi-serv)# no supplementary-service sip refer` or `Router(config-dial-peer)# no supplementary-service sip refer`	Disables SIP call forwarding or call transfer supplementary services globally or for a dial peer. • **moved-temporarily**—SIP redirect response for call forwarding. • **refer**—SIP REFER message for call transfers. • Sending REFER and redirect messages to the destination is the default behavior. **Note** This command is supported for calls between SIP phones and calls between SCCP phones. It is not supported for a mixture of SCCP and SIP endpoints.
Step 5	`end` **Example:** `Router(config-voi-serv)# end` or `Router(config-dial-peer)# end`	Exits to privileged EXEC mode.

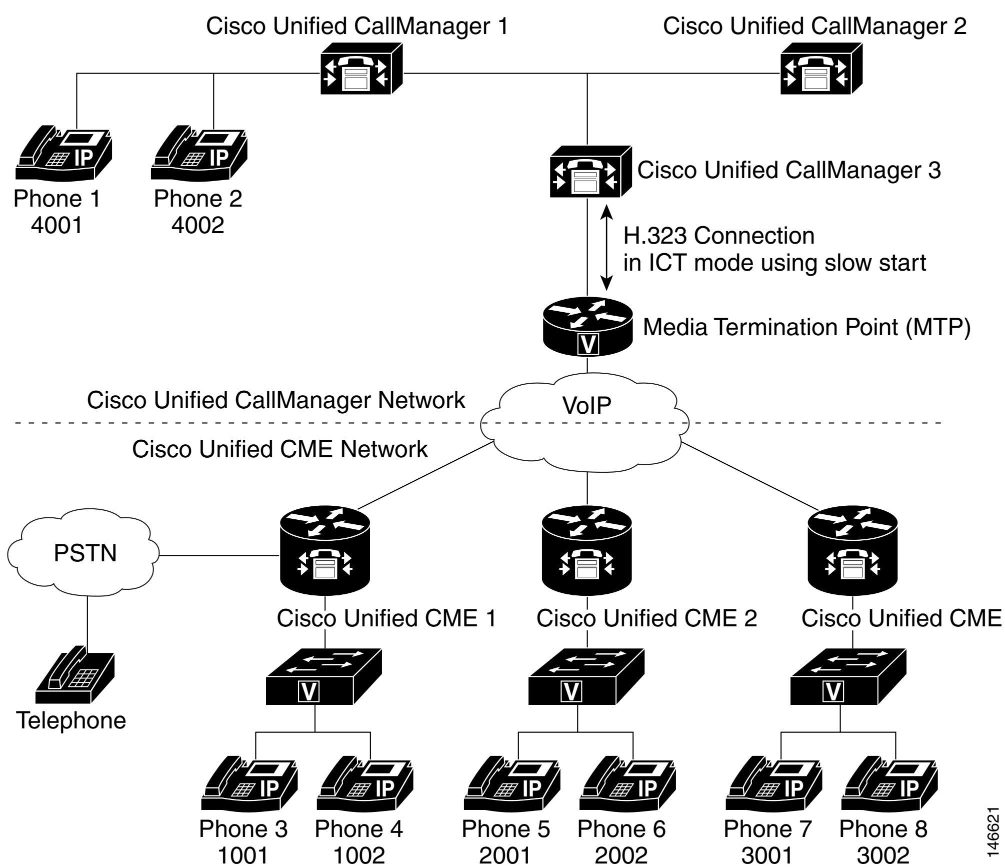
Enabling Interworking with Cisco Unified Communications Manager

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:

- Configuring Cisco CME 3.1 or Later to Interwork with Cisco Unified Communications Manager, page 559
- Enabling Cisco Unified Communications Manager to Interwork with Cisco Unified CME, page 562
- Troubleshooting Transfer and Forwarding Configuration, page 562

Figure 33 shows a network containing Cisco Unified CME and Cisco Unified Communications Manager systems.

Figure 33 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 the "Forwarding Calls Using Local Hairpin Routing" section on page 551.

Configuring Cisco CME 3.1 or Later to Interwork with Cisco Unified Communications Manager

All of the Cisco IOS 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 nondefault 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.

	Command or Action	Purpose
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 a Cisco Unified Communications Manager and exchange calls with it. This is the default. • 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 the Cisco Unified Communications Manager to generate local ringback for calls to Cisco Unified CME phones. This is the default. • 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. • 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.

	Command or Action	Purpose
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.
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. • 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. • 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. • 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`	Returns to privileged EXEC mode.

What to Do Next

Set up Cisco Unified Communications Manager using the configuration procedure in the "Enabling Cisco Unified Communications Manager to Interwork with Cisco Unified CME" section on page 562.

Enabling Cisco Unified Communications Manager to Interwork with Cisco Unified CME

To enable Cisco Unified Communications Manager to interwork with a Cisco CME 3.1 or later system, perform the following steps in addition to the normal Cisco Unified Communications Manager configuration.

SUMMARY STEPS

1. Set Cisco Unified Communications Manager service parameters.
2. Configure the Cisco CME 3.1 or later system as an ICT in the Cisco Unified Communications Manager network.
3. Ensure that the Cisco Unified Communications Manager network uses an MTP.
4. Set up dial peers to establish routing.

DETAILED STEPS

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 the Cisco CME 3.1 or later system as an ICT in the Cisco Unified Communications Manager network. For information about different intercluster trunk types and configuration instructions, see the 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 the Cisco CME 3.1 or later system. All media streams between Cisco Unified Communications Manager and Cisco CME 3.1 or later must pass through the MTP because Cisco CM 3.1 does not support transcoding. For more information, see the 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 Transfer and Forwarding 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
```

SIP: Configuring 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.

Prerequisites

- 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 the "Enabling Calls in Your VoIP Network" on page 110.
- Cisco CME 3.4 or a later version.

Restrictions

- 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.

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 noan** *directory-number* **timeout** *seconds*
8. **call-forward b2bua unreachable** *directory-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.

	Command or Action	Purpose
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.
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 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. • **timeout** *seconds*—Duration that a call can ring before it is forwarded to the destination directory number. Range: 3 to 60000. Default: 20.

	Command or Action	Purpose
Step 8	**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 9	**end** **Example:** `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

SIP: Configuring Call-Forwarding-All Soft Key URI

To specify the uniform resource identifier (URI) for the call forward all (CfwdAll) soft key 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.

Prerequisites

- 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 "SIP: Configuring SIP-to-SIP Phone Call Forwarding" on page 564.

Restrictions

- 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 soft key, it is enabled on the primary line.

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.
Step 5	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

SIP: Specifying Number of 3XX Responses To be Handled

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.

Prerequisites

- 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.
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 configuration mode and enters privileged EXEC mode.

SIP: Configuring Call Transfer

To create and apply a template to enable call transfer softkeys on an individual SIP phone in Cisco Unified CME, perform the following steps.

Prerequisites

Cisco CME 3.4 or a later version.

Restrictions

- 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 "SCCP: Modifying Soft-Key Display" on page 878.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **voice register template** *template-tag*
4. **transfer-attended**
5. **transfer-blind**
6. **voice register template** *template-tag*
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 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	`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.

	Command or Action	Purpose
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 configuration mode and enters privileged EXEC mode.

Configuration Examples for Call Transfer and Forwarding

The following configuration examples are included in this section:

H.450.2 and H.450.3: Example

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
```

Basic Call Forwarding: Example

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
```

Call Forwarding Blocked for Local Calls: Example

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
```

Selective Call Forwarding: Example

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
```

Call Transfer: Example

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
```

H.450.12: Example

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
```

H.450.7 and QSIG Supplementary Services: Example

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
```

Cisco Unified CME and Cisco Unified Communications Manager in Same Network: Example

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
```

H.450 Tandem Gateway Working with Cisco Unified CME and Cisco Unified Communications Manager: Example

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
```

Forwarding Calls to Cisco Unity Express: Example

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
```

Where to Go Next

If you are finished modifying the configuration, generate a new configuration file and restart the phones. See "Generating Configuration Files for Phones" on page 265.

Soft Keys

To block the function of the call-forward-all or transfer soft key without removing the key display or to remove the soft key from one or more phones, see the "How to Customize Soft Keys" section on page 878.

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 "Configuring Feature Access Codes" on page 775.

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 "Configuring Call-Coverage Features" on page 581.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Call Transfer and Forwarding

Table 30 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 30 lists the 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.

Table 30 Feature Information for Call Transfer and Forwarding

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	• 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.

Table 30 Feature Information for Call Transfer and Forwarding

Feature Name	Cisco Unified CME Version	Feature Information
Call Forwarding	1.0	Call forwarding for all calls, busy conditions, and no-answer conditions was introduced, using a Cisco-proprietary method.
Call Transfer	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	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.

Configuring Call-Coverage Features

Last Updated: June 18, 2007

This chapter describes features that can be used to provide appropriate, flexible coverage for incoming calls in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Call Coverage" section on page 654.

Contents

Information About Call Coverage Features

To configure call coverage features, you should understand the following concepts:

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 directory number 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 31 summarizes call-coverage features.

Table 31 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.	SCCP: Enabling Call Forwarding for a Directory Number, page 541 or SIP: Configuring SIP-to-SIP Phone Call Forwarding, page 564
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.	SCCP: Configuring Call Hunt, page 604 or SIP: Configuring Call Hunt, page 607
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.	SCCP: Creating Pickup Groups, page 609
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.	SCCP: Configuring Call-Waiting Indicator Tone, page 611 or SIP: Enabling Call Waiting, page 613

Table 31 Call-Coverage Feature Summary (continued)

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.	SCCP: Configuring Hunt Groups, page 614 or SIP: Configuring Hunt Groups, page 623.
Night Service	Calls to ephone-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.	SCCP: Configuring Night Service, page 627.
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.	SCCP: Configuring Overlaid Ephone-dns, page 633.

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 the "SCCP: Configuring Call Hunt" section on page 604 and the "SIP: Configuring Call Hunt" section on page 607.

Call Pickup

Call pickup, and pickup groups, enable phone users to answer a call that is ringing on a different directory number other than their own. If both numbers to be answered are in the same pickup group, the user presses fewer keys to pick up the call.

Call pickup has the following variations:

- Directed Call Pickup—Call pickup, explicit ringing extension. Any local phone user can pick up a call that is on hold on another directory number in Cisco Unified CME. Phone user does not need to belong to a pickup group to use this method. This is a default behavior.
- Group Pickup, Different Group—Call pickup, explicit group ringing extension. Phone user can answer a ringing phone in any pickup group if the user knows the group number of the ringing phone. If there is only one pickup group defined in Cisco Unified CME, the phone user can pick up the call by pressing a soft key. Phone user does not need to belong to a pickup group to use this method.
- Local Group Pickup—Call pickup, local group ringing extension. Phone users can pick up the called number on another phone by pressing a soft key plus an asterisk (*) their own phone if both phones are in the same pickup group.

Administrators can assign each ephone-dn independently to a maximum of one pickup group. There is no limit to the number of ephone-dns that can be assigned to a single pickup group, and there is no limit to the number of pickup groups that can be defined in a Cisco Unified CME system.

Pickup group numbers may be of varying length, but must have unique leading digits. For example, you cannot define pickup group 17 and pickup group 177 for the same Cisco Unified CME system because a pickup in group 17 will always be triggered before the user can enter the final 7 for 177.

Figure 34 shows four call-pickup scenarios.

Figure 34 Call Pickup

For configuration information, see the "SCCP: Creating Pickup Groups" section on page 609.

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 the "SCCP: Configuring Call-Waiting Indicator Tone" section on page 611.

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 the "SIP: Enabling Call Waiting" section on page 613.

For information on call waiting using Overlaid ephone-dns, see the "Overlaid Ephone-dns" section on page 599.

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 32 shows the possible beep behaviors of one ephone-dn calling another ephone-dn that is connected to another caller.

Table 32 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
—	`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 accept` `no 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

Table 32 Call-Waiting Beep Behavior (continued)

Ephone-dn 1 Configuration	Ephone-dn 2 Configuration	Active Call on DN	Incoming Call on DN	Expected Behavior
`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 the "SCCP: Configuring Call-Waiting Indicator Tone" section on page 611 or the "SIP: Enabling Call Waiting" section on page 613.

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 directory numbers. Each hunt group can include up to 20 member directory numbers.

Incoming calls are redirected from a hunt group pilot number to the first directory number as defined by the configuration. If the first directory 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 directory number to directory number in the list until it is answered or until the call reaches the number that was 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.

For information on displaying hunt group statistics, 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 directory number that rings for successive calls to the hunt group pilot number. Hunt group types include the following:

- Sequential Hunt Groups—Directory 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.
- Peer Hunt Groups—The first directory 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.
- Longest-Idle Hunt Groups—Calls go first to the directory 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.
- Parallel Hunt Groups—Calls ring all directory numbers in the hunt group simultaneously.

The number that is defined as the final number for a hunt group may also be the pilot number for another hunt group (with suitable protection to avoid infinite loops). If a final number is assigned as the pilot number of a second hunt group, the pilot number of the first hunt group cannot be configured as a final number in any hunt group. If there is a third hunt group, the second hunt group cannot be configured as a final number, and so forth.

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 will disconnect.

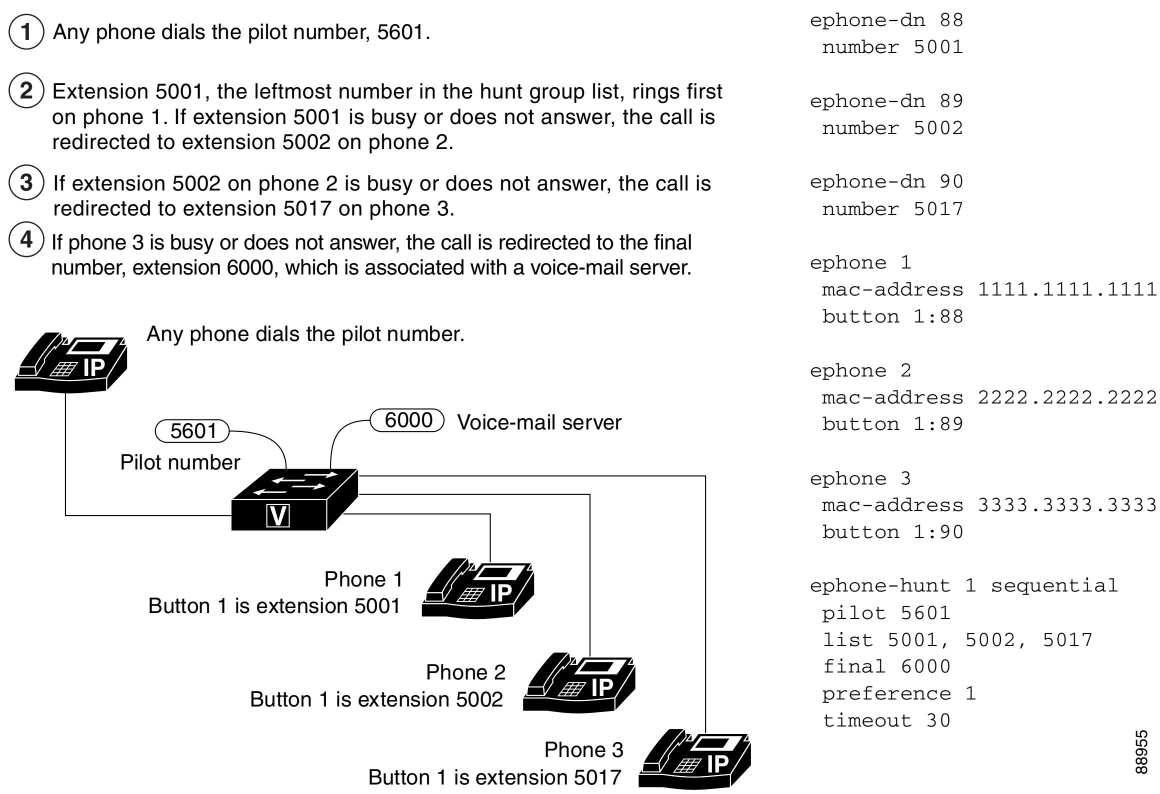
```
ephone-hunt 1 sequential
 pilot 8000
 list 8001, 8002, 8003, 8004
 final 9000
ephone-hunt 2 sequential
 pilot 9000
 list 9001, 9002, 9003, 9004
 final 7000
ephone-hunt 3 sequential
 pilot 7000
 list 7001, 7002, 7003, 7004
 final 5000
```

Figure 35 on page 589 illustrates a sequential hunt group, Figure 36 on page 590 illustrates a peer hunt group, and Figure 37 on page 591 illustrates a longest-idle hunt group.

Sequential Hunt Groups

In a sequential hunt group, directory 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 35 Sequential hunt Group



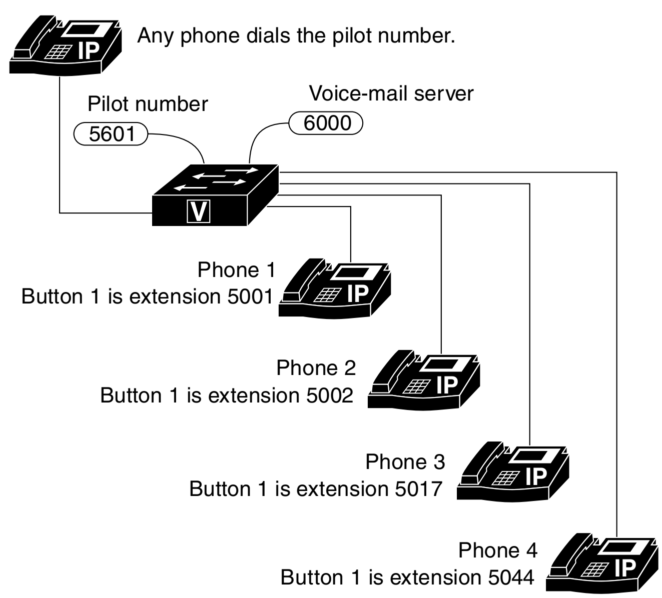
Peer Hunt Groups

In a peer hunt group, the first directory 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 when the hunt group was defined.

Figure 36 illustrates a peer hunt group.

Figure 36 Peer hunt Group

1. Any phone dials the pilot number, 5601, which is not associated with a physical phone instrument.
2. Extension 5017 on phone 3 is selected to ring first because extension 5002 was the last number to ring the last time that the pilot number was called.
3. If extension 5017 is busy or does not answer, the call is redirected to extension 5044 on phone 4 (first hop).
4. If extension 5044 is busy or does not answer, the call is redirected to extension 5001 on phone 1 (second hop).
5. If extension 5001 is busy or does not answer, the call has reached the maximum number of hops (3), and it is redirected to the final number, extension 6000, which is associated with a voice-mail server.




```
ephone-dn 88
 number 5001

ephone-dn 89
 number 5002

ephone-dn 90
 number 5017

ephone-dn 91
 number 5044

ephone 1
 mac-address 1111.1111.1111
 button 1:88

ephone 2
 mac-address 2222.2222.2222
 button 1:89

ephone 3
 mac-address 3333.3333.3333
 button 1:90

ephone 4
 mac-address 4444.4444.4444
 button 1:91

ephone-hunt 1 peer
 pilot 5601
 list 5001, 5002, 5017, 5044
 final 6000
 hops 3
 preference 1
 timeout 30
 no-reg
```

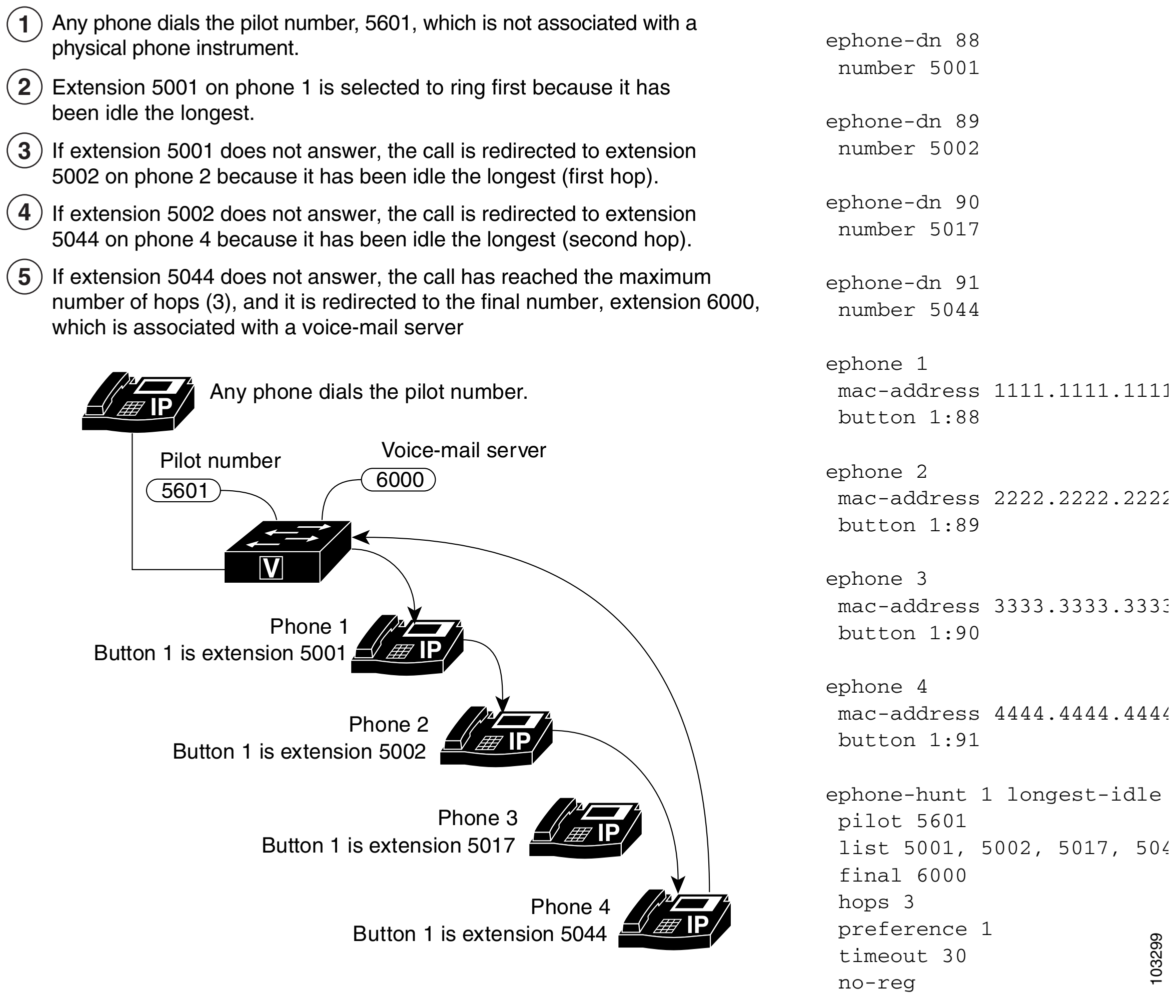
Longest-Idle Hunt Groups

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 37 illustrates a longest-idle hunt group.

Figure 37 Longest-Idle hunt Group



Parallel Hunt Groups

In a parallel hunt group, calls simultaneously ring multiple phones. The use of parallel hunt groups is also referred to as application-level forking because it enables the forking of a call to multiple destinations. Parallel hunt group are supported by SIP phones only. (To enable similar functionality on SCCP phones, use the ephone-dn overlay feature for shared lines. See the "Shared-Line Overlays" section on page 600.)

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 the "SIP: Configuring Hunt Groups" section on page 623.

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 33 compares the following agent availability features:

- Dynamic Hunt Group Membership, page 595
- Agent Status Control, page 595
- Automatic Agent Status Not-Ready, page 596

Table 33 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.
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.

Table 33 Comparison of Hunt Group Agent Availability Features (continued)

Comparison Factor	Dynamic Membership	Agent Status Control	Automatic Agent Status Not-Ready
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 ephone FAC or the HLog ephone-dn 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 SCCP: Configuring Hunt Groups, page 614.	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 SCCP: Configuring Hunt Groups, page 614.	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 SCCP: Configuring Hunt Groups, page 614.
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 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 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 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 hunt groups.

To dynamically join a hunt group, a phone user dials a standard or custom FAC for joining a hunt group. The standard FAC to join a hunt group is *3. If multiple hunt groups have been created that allow dynamic membership, the phone user must also dial the hunt group pilot number. For example, if the following hunt groups are defined, a phone user dials *38000 to join the Sales hunt group:

```
ephone-hunt 24 sequential
 pilot 8000
 list 8001, 8002, *, *
 description Sales Group
 final 9000

ephone-hunt 25 sequential
 pilot 7000
 list 7001, 7002, *, *
 description Service Group
 final 9000
```

To leave a hunt group, a phone user dials the standard or custom FAC for leaving a hunt group. The standard FAC to leave a hunt group is #3. See “Customizing Soft Keys” on page 875.

Note The Dynamic Membership feature is different from the Agent Status Control feature and the Automatic Agent Status Not-Ready feature. Table 33 on page 593 compares the features.

Agent Status Control

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 must be used 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, page 651.

Note The Agent Status Control feature is different from the Dynamic Membership feature and the Automatic Agent Status Not-Ready feature. Table 33 on page 593 compares the features.

Automatic Agent Status Not-Ready

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 33 on page 593 compares the features.

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 to phones that have been specified to receive this special ring (the phones are known as night-service phones). 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 (Figure 38).

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 because the PSTN connection to the Cisco Unified CME system does not support Direct Inward Dialing (DID). 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.

If optionally configured, night service can be manually toggled on and off from any phone that has a line that is designated as a night-service line. When night service is active, a message is displayed on the night-service phones.

Night service requires that you define the following parameters:

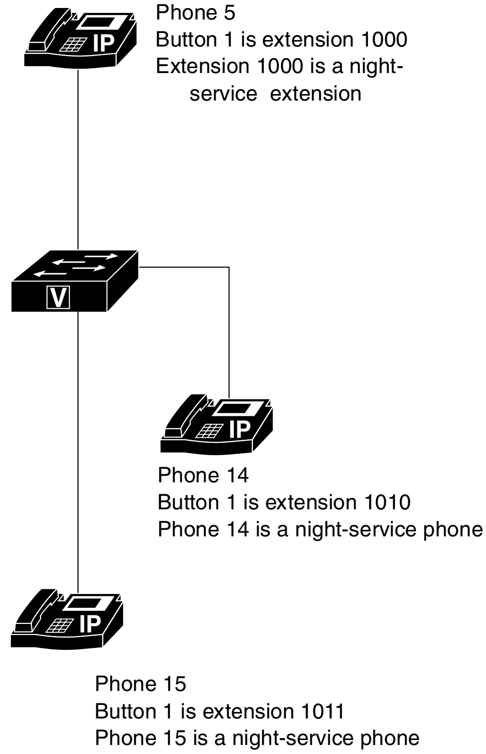
1. Night-service time period—Day or date and hours during which night service is active. Step 4 to Step 8 in the following procedure define the night-service period.
2. Night-service extensions (directory numbers)—When a night-service extension receives an incoming call during the night-service period, night-service notification is triggered. Step 12 in the following procedure specifies night service for an directory number.
3. Night-service notification phones (ephones)—Night-service notification phones are alerted with a distinctive ring when incoming calls are received on night-service lines during the night-service time period. The night-service notification phone user can answer the call using call pickup or group call pickup. Step 15 in the following procedure assigns night-service notification to a phone. This phone receives a distinctive alerting ring and notification display when a night-service extension receives an incoming call.
4. (Optional) Night-service toggle code—A code to allow night-service treatment to be manually toggled off and on from any phone that has a line assigned to night service. Before Cisco CME 3.3, using the night-service code turned night service on or off only for directory numbers on the phone at which the code was 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. The following procedure defines a night-service toggle code.

Figure 38 illustrates night service.

Figure 38 Night Service

1. Extension 1000 has been designated as a night-service extension (ephone-dn). When extension 1000 receives an incoming call during a night-service period, phone 5 rings and notification is made to the night-service phones.

2. Phones 14 and 15 have been designated as night-service phones. When phone 5 starts ringing, phones 14 and 15 ring once and display "Night Service 1000." The incoming call on extension 1000 can be answered from phone 14 or phone 15 using call pickup.




```
telephony-service
 night-service day fri 17:01 17:00
 night-service day sat 17:01 17:00
 night-service day sun 17:01 07:59
 night-service date jan 1 00:00 00:00
 night-service code *1234
!
ephone-dn 1
 number 1000
 night-service bell
!
ephone-dn 10
 number 1010
!
ephone-dn 11
 number 1011
!
ephone 5
 mac-address 1111.2222.0001
 button 1:1
!
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
```

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.

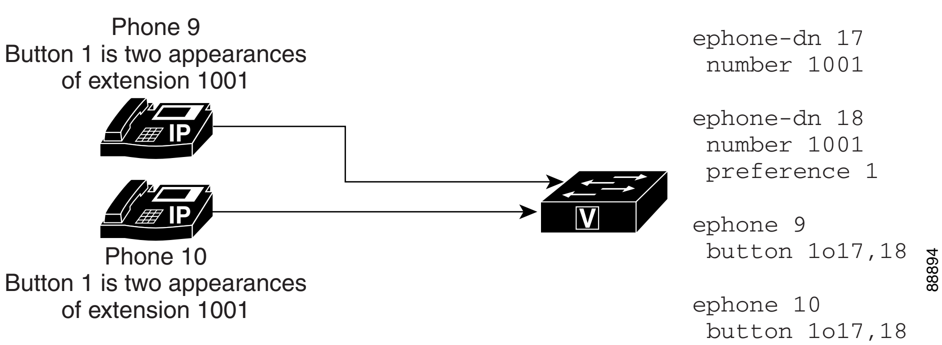
The order in which overlaid ephone-dns are used by incoming calls can be determined by the call hunt commands, **preference** and **huntstop**. For example, ephone-dn 1 to ephone-dn 4 have the same extension number, 1001. Three phones are configured with the **button 1o1,2,3,4** command. A call to 1001 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 the "Call Hunt" section on page 583.

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 39 on page 599 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 39 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
```

For a more detailed example, see the "Shared-line Overlaid Ephone-dns: Example" section on page 646.

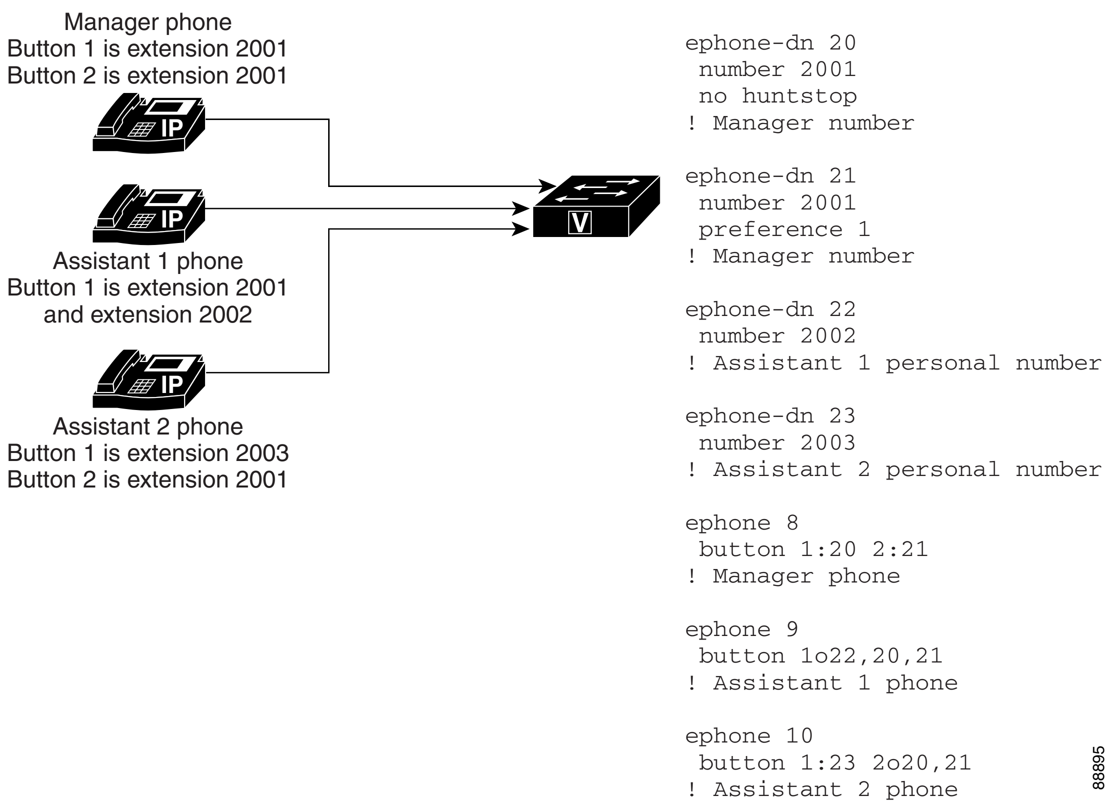
A more complex directory number configuration mixes overlaid directory numbers with shared directory numbers and plain dual-line directory numbers on the same phones. Figure 40 on page 601 illustrates the following example of a manager with two assistants. On the manager's phone the same number, 2001, 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 40 Overlaid Ephone-dn (Complex Case)



For configuration information, see the "SCCP: Configuring Overlaid Ephone-dns" section on page 633.

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 the "SCCP: Configuring Overlaid Ephone-dns" section on page 633.

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 the "SCCP: Configuring Call-Waiting Indicator Tone" section on page 611.) 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 the "SCCP: Configuring Call-Waiting Indicator Tone" section on page 611.

Extending 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 the "SCCP: Configuring Overlaid Ephone-dns" section on page 633.

How to Configure Call Coverage Features

This section contains the following procedures:

Call Hunt

Call Pickup

Call Waiting

Hunt Groups

- SIP: Configuring Hunt Groups, page 623 (required)

Night Service

- SCCP: Configuring Night Service, page 627 (required)
- SCCP: Verifying Night Service, page 631 (optional)

Overlaid Ephone-dns

- SCCP: Configuring Overlaid Ephone-dns, page 633 (required)
- SCCP: Verifying Overlaid Ephone-dns, page 636 (optional)

SCCP: Configuring Call Hunt

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. **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.

	Command or Action	Purpose
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 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. • 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 an ephone-dn if the first channel is busy or does not answer. • Required for dual-line ephone-dns.
Step 8	**end** **Example:** `Router(config-ephone-dn)# end`	Returns to 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.*

SCCP: Verifying Call Hunt

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.

```
Router# show telephony-service ephone-dn

ephone-dn 243
 number 1233
 preference 1
 huntstop
```

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
```

SIP: Configuring Call Hunt

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* **Example:** `Router(config-register-dn)# number 5001`	Associates a phone number with the directory number. • 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.

	Command or Action	Purpose
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.*

SCCP: Enabling Local-Group Call Pickup at a System-Level

To enable local-group call pickup at a system-level, and disable directed call pickup, perform the following steps.

Note To selectively disable directed call pickup for one or more SCCP phones, use the **features blocked** command in ephone-template mode. For configuration information, see "SCCP: Enabling Ephone Templates" on page 929.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **no service directed-pickup**
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	**no service directed-pickup** **Example:** `Router(config-telephony)# no service directed-pickup`	Disables directed call pickup. • Changes the action of the PickUp soft key to perform local group call pickup rather than directed call pickup.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Creating Pickup Groups

To create a pickup group, perform the following steps.

Prerequisites

Directory numbers to be added to a pickup group must be configured in Cisco Unified CME. For configuration information, see "SCCP: Creating Directory Numbers" on page 177.

Restrictions

- Each directory number can be independently assigned to a maximum of one pickup group.
- There is no limit to the number of directory numbers that can be assigned to a single pickup group.
- There is no limit to the number of pickup groups that can be defined in Cisco Unified CME.
- Pickup group numbers may be of varying length, but must have unique leading digits.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]
4. **pickup-group** *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-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	**pickup-group** *number* **Example:** `Router(config-ephone-dn)# pickup-group 2345`	Creates a pickup group and assigns the directory number being configured to the group. • *number*—Digit string of up to 32 characters. Group numbers may be of varying length, but they must have unique leading digits. For example, if there is a group number 17, there cannot also be a group number 177.
Step 5	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 6	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Verifying Call Pickup

Step 1 Use the **show running-config** command to verify your configuration. Call pickup groups are listed in the ephone-dn portion of the output.

```
Router# show running-config
!
ephone-dn  34  dual-line
 ring feature secondary
 number 330 secondary 331
 pickup-group 30
 call-forward noan 500 timeout 10 secondary
 huntstop channel
 no huntstop
```

Step 2 Use the **show telephony-service ephone-dn** command to display call pickup configuration information.

```
Router# show telephony-service ephone-dn

ephone-dn 2
 number 5002
 pickup group 30
 call-forward noan 5001 timeout 8
```

SCCP: Configuring Call-Waiting Indicator Tone

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.

Restrictions

- 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 the "SCCP: Assigning Directory Numbers to Phones" on page 179.
- 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).
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.

SCCP: Verifying Call-Waiting Indicator Tone

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.

```
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.

```
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
```

SIP: Enabling Call Waiting

To enable call waiting on an individual SIP phone, perform the following steps.

Prerequisites

- 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** **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)# 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.

SCCP: Configuring Hunt Groups

To define a hunt group and optional agent availability parameters, perform the following steps.

Prerequisites

Directory numbers to be included in a hunt group must be already configured in Cisco Unified CME. For configuration information, see "SCCP: Creating Directory Numbers" on page 177.

Restrictions

- 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 VG 224.
- Shared ephone-dns cannot use the Agent Status Control or Automatic Agent Not-Ready feature.
- The Agent Status Control feature and the HLog soft key require the user locale to be set to US. To display the HLog soft key on a Cisco Unified IP Phone 7940 or Cisco Unified IP Phone 7960, change the user locale to any locale other than US and reset the phone. Then change the user locale to US and reset the phone again.

- If directory numbers that are members of a hunt group are to be 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.

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** | *agent-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**} **Example:** `Router(config)# ephone-hunt 23 peer`	Enters ephone-hunt configuration mode to define an ephone hunt group. • *hunt-tag*—Unique sequence number that identifies this hunt group during configuration tasks. Range: 1 to 100. • **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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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 9.
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. • **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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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 5. **Note** This command is required if the number of hops is greater than 5.
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 soft key 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 if 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.
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.

SCCP: Verifying Hunt Groups

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.

```
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.

```
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.

```
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
```

SIP: Configuring Hunt Groups

To redirect calls for a specific number (hunt-group pilot number) to a defined group of directory numbers on SIP phones, perform the following steps.

Prerequisites

Directory numbers to be added to a hunt group must be configured in Cisco Unified CME. For configuration information, see "SIP: Creating Directory Numbers" on page 181.

Restrictions

- SIP-to-H.323 calls are not supported.
- If call forward is configured for a hunt group member, call forward is ignored by the hunt group.
- Forwarding or transferring to a voice hunt group is not supported.

- Voice-class with codec list can be configured under voice register pool, and more than one list member will not be supported for B2BUA call.
- Caller ID update is not supported for supplementary services.
- 100 voice hunt groups is the maximum number of hunt group supported.
- Voice hunt groups are subject to max-redirect restriction.
- A pilot dial peer cannot be used as a voice hunt group and a hunt group at the same time.
- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice hunt-group** *hunt-tag* [**longest-idle** | **parallel** | **peer** | **sequential**]
4. **pilot** *number* [**secondary** *number*]
5. **list** *dn-number*, *dn-number*[, *dn-number...*]
6. **final** *final-number*
7. **preference** *preference-order* [**secondary** *secondary-order*]
8. **hops** *number*
9. **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.

	Command or Action	Purpose
Step 3	**voice hunt-group** *hunt-tag* [**longest-idle** | **parallel** | **peer** | **sequential**] **Example:** `Router(config)# voice hunt-group 1 longest-idle`	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. • **longest idle**—Hunt group in which calls go to the directory number that has been idle for the longest time. • **parallel**—Hunt group in which calls simultaneously ring multiple phones. • **peer**—Hunt group in which the first directory number is selected round-robin from the list. • **sequential**—Hunt group in which directory numbers ring in the order in which they are listed, left to right. • To change the hunt-group type, remove the existing hunt group first by using the **no** form of the command; then, recreate the group.
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** *directory-number, directory-number* [,*directory-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. • *directory-numbers*—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.

	Command or Action	Purpose
Step 6	**final** *directory-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.
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 10 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 0 to 10, where 0 is the highest preference and 10 is the lowest preference. Default is 9.
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	**end** **Example:** `Router(config-voice-hunt-group)# end`	Exits configuration mode and enters privileged EXEC mode.

SCCP: Configuring Night Service

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.

Restrictions

In Cisco Unified CME 4.0 and later, 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. **exit**
11. **ephone-dn** *dn-tag*
12. **night-service bell**
13. **exit**
14. **ephone** *phone-tag*
15. **night-service bell**
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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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. Weekend is defined as 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. The night-service state is indicated in a display message on phones that have active night-service lines. • *digit-string*—String of up to 16 keypad digits. The code must begin with an asterisk (*).
Step 10	**exit** **Example:** `Router(config-telephony)# exit`	Exits telephony-service configuration mode.
Step 11	**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. • *dn-tag*—Unique sequence number that identifies the ephone-dn to receive night-service treatment.
Step 12	**night-service bell** **Example:** `Router(config-ephone-dn)# night-service bell`	Marks this ephone-dn for night-service treatment. Incoming calls to this ephone-dn during the night-service time period send an alert notification to all IP phones that are marked to receive night-service bell notification.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Router(config-ephone-dn)# exit`	Exits ephone-dn configuration mode.
Step 14	**ephone** *phone-tag* **Example:** `Router(config)# ephone 12`	Enters ephone configuration mode. This is a phone that will be notified when an incoming call is received by a night-service ephone-dn during a night-service period. • *phone-tag*—The unique sequence number of the phone that you are designating as a night-service phone.
Step 15	**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. The alert notification is a splash ring that is not associated with any of the individual lines on the IP phone and a visual display of the ephone-dn line number. The phone user can pick up the call by executing a PickUp or GPickUp.
Step 16	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

SCCP: Verifying Night Service

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.

```
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 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.

```
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
```

SCCP: Configuring Overlaid Ephone-dns

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.

Restrictions

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag* [**dual-line**]

4. **number** *number*
5. **preference** *preference-value*
6. **huntstop**
   or
   no huntstop
7. **call-forward noan**
8. **call-forward busy**
9. **huntstop channel**
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.
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.

	Command or Action	Purpose
Step 6	**no huntstop** or **huntstop** **Example:** `Router(config-ephone-dn)# no huntstop` or **Example:** `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	**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 8	**call-forward busy**	(Optional) Forwards incoming call if line is busy. • Set this command on the last ephone-dn in the overlay set only.
Step 9	**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 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.

	Command or Action	Purpose
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.

SCCP: Verifying Overlaid Ephone-dns

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.

```
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)
```

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.

Configuration Examples for Call Coverage Features

This section contains the following configuration examples:

Call Hunt: Examples

This section contains the following examples:

Ephone-dn Dial-Peer Preference: Example

The following example sets an ephone-dn preference number of 2 for the primary number of the ephone-dn with dn-tag 3:

```
ephone-dn 3
 number 3001
 preference 2
```

Huntstop Disabled: Example

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
```

Channel Huntstop: Example

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
```

SIP Call Hunt: Example

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
```

Call Pickup: Examples

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
```

Call-Waiting Beep: Example

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
```

Call-Waiting Ring: Example

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
```

Hunt Group: Examples

This section contains the following examples:

- Sequential Ephone Hunt Group: Example, page 640
- Peer Ephone Hunt Group: Example, page 641
- Longest-Idle Ephone Hunt Group: Example, page 641
- Longest-Idle Ephone Hunt Group Using From-Ring Option: Example, page 641
- Logout Display: Example, page 642
- Dynamic Membership: Example, page 642
- Agent Status Control: Example, page 642
- Automatic Agent Not-Ready: Example, page 643

Sequential Ephone Hunt Group: Example

The following example defines a sequential ephone hunt group with the pilot number 5601 and the final number 6000, with four numbers in the list of phones that answer for the pilot number.

```
ephone-hunt 2 sequential
 pilot 600
 list 621, *, 623
 final 5255348
 max-timeout 10
 timeout 20, 20, 20
 fwd-final  orig-phone
```

Peer Ephone Hunt Group: Example

The following example defines peer ephone hunt group 10 with a pilot number 450, a final number 500, and eight 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
```

Longest-Idle Ephone Hunt Group: Example

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
```

Longest-Idle Ephone Hunt Group Using From-Ring Option: Example

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
```

Logout Display: Example

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
```

Dynamic Membership: Example

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
```

Agent Status Control: Example

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 soft keys 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
```

Automatic Agent Not-Ready: Example

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
```

Night Service: Examples

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
```

Overlaid Ephone-dns Examples

This section contains the following examples:

- Overlaid Ephone-dn: Example, page 645
- Overlaid Dual-Line Ephone-dn: Example, page 645
- Shared-line Overlaid Ephone-dns: Example, page 646
- Overlaid Ephone-dn with Call Waiting: Example, page 647
- Overlaid Ephone-dns with Rollover Buttons: Example, page 648
- Called Directory Name Display for Overlaid Ephone-dns: Example, page 648
- Called Ephone-dn Name Display for Overlaid Ephone-dns: Example, page 650

Overlaid Ephone-dn: Example

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
```

Overlaid Dual-Line Ephone-dn: Example

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
```

Shared-line Overlaid Ephone-dns: Example

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
```

Overlaid Ephone-dn with Call Waiting: Example

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
```

Overlaid Ephone-dns with Rollover Buttons: Example

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
```

Called Directory Name Display for Overlaid Ephone-dns: Example

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 “Configuring Directory Services” on page 707.

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 the "Hunt Groups" section on page 587. 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 number 5100 secondary 555....
 list 1001, 1002, 1003, 1004
 final number 5556000
 hops 5
 preference 1
 timeout 20
 no-reg
```

Called Ephone-dn Name Display for Overlaid Ephone-dns: Example

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 "Configuring Directory Services" on page 707.

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
```

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 "Configuring Directory Services" on page 707.

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.

For more information, see "Customizing Soft Keys" on page 875.

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 "Configuring Feature Access Codes" on page 775.

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 Configuring Call Blocking, page 485.

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 "Customizing Soft Keys" on page 875.

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 "Creating Templates" on page 927.

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*.

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 "Configuring Do Not Disturb" on page 727.

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 the "SCCP: Enabling Call Forwarding for a Directory Number" section on page 541.

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 "Creating Templates" on page 927.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Call Coverage Features

Table 34 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified Communications Manager Express and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 34 lists the 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.

Table 34 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. • Channel huntstop was introduced.
	1.0	• Ephone-dn dial-peer preference was introduced. • Huntstop was introduced.
Call Pickup	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	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.

Table 34 Feature Information for Call Coverage

Feature Name	Cisco Unified CME Version	Modification
Hunt Groups	4.0	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 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 hunt group. • 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.

Table 34 Feature Information for Call Coverage

Feature Name	Cisco Unified CME Version	Modification
	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	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	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.
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.

Configuring Caller ID Blocking

Last Updated: March 26, 2007

This chapter describes the caller-ID (CLID) blocking feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Caller ID Blocking" section on page 664.

Contents

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

To enable Caller ID Blocking, you should understand the following concept:

- Caller ID Blocking on Outbound Calls, page 658

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.

How to Configure Caller ID Blocking

This section contains the following tasks:

- Blocking Caller ID For Local Calls From a Directory Number, page 658 (optional)
- Blocking Caller ID For All Outbound Calls, page 660 (optional)
- Verifying Caller ID Blocking, page 661 (optional)

Blocking Caller ID For Local Calls From a Directory Number

To define a code that phone users can dial to block caller ID display on all local calls from a particular ephone-dn, 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.
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 all caller-ID information for outbound calls that originate from this ephone-dn. • By default, caller ID is not blocked on calls that originate from a Cisco Unified IP phone. • This command tells the far-end gateway device to block display of calling-party information for the calls received from this ephone-dn.
Step 8	**end** **Example:** `Router(config-dial-peer)# end`	Returns to privileged EXEC mode.

Blocking Caller ID For All Outbound Calls

To block the CLID name or number on outbound VoIP calls from a particular dial peer, perform the following steps.

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.
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.

Verifying Caller ID Blocking

Step 1 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.

```
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

This section contains the following examples:

- Caller ID Blocking Code: Example, page 662
- Caller ID Blocking for Outbound Calls: Example, page 662

Caller ID Blocking Code: Example

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
```

Caller ID Blocking for Outbound Calls: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Caller ID Blocking

Table 35 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 35 lists the 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.

Table 35 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.

Configuring Conferencing

Last Updated: September 10, 2007

This chapter describes the conferencing support in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Conferencing" section on page 705.

Contents

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

To enable conferencing, you should understand the following concepts:

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 are created when one party calls another party, then either party adds one or more parties to the conference call. Ad hoc conferences can be hardware-based or software-based, depending on the number of parties. Hardware-based ad hoc conferencing uses digital signal processors (DSPs) to allow more parties than software-based ad hoc conferencing, which allows three parties only.

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.

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 the "Transcoding When a Remote Phone Uses G.729r8" section on page 325.

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.

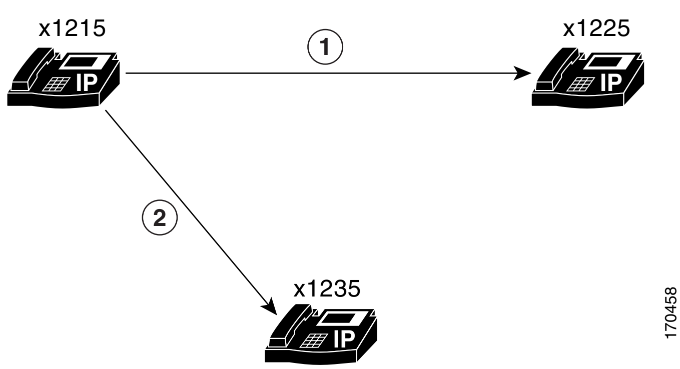
In Cisco Unified CME 4.0 and later versions, behavior for the end of three-way conferences can be configured at a phone level. The options specify whether the last party that joined a conference can be dropped from the conference and whether the remaining two parties should be allowed to continue their 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, 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 41 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 41 Simple Ad Hoc 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.

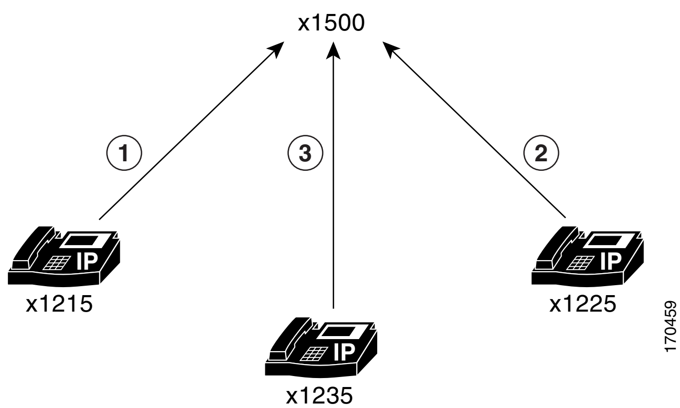
You can configure conferencing so that the conference drops when the creator hangs up, and you can configure it so that the conference drops when the last local party hangs up. The default is that the conference is not dropped, regardless of whether the creator hangs up, provided three parties remain in the conference.

For configuration information, see the "SCCP: Configuring Conferencing Options for a Phone" section on page 685 for more information.

Meet-Me Conferencing

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 42 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 42 Simple Meet-Me Conference Scenario



Configuring 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 the "SCCP: Configuring the DSP Farm" section on page 679 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.

Soft Keys for Conference Functions

In Cisco Unified CME 4.1 and later versions, the following soft keys provide conferencing functions for multi-party conferencing enhancements on your phone:

- ConfList—Conference list. Lists all parties in a conference. For 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.
- Join—Joins an established call to conference. After you press **Select** to choose an established call or conference, press **Join** to join that call or conference to the established call or 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 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. This soft key is pressed by the creator before dialing the conference number. Other meet-me conference parties dial the conference number only to join the conference. This soft key must be configured before you can initiate meet-me conferences.

How to Configure Conferencing

This section contains the following tasks:

Three-Party Ad Conferencing

- Modifying the Default Configuration for Three-Party Ad Hoc Conferencing, page 669 (optional)
- SCCP: Configuring Conferencing Options on a Phone, page 671 (optional)
- SIP: Configuring Conferencing Options on a Phone, page 673 (optional)

Multi-Party Ad Hoc and Meet-Me Conferencing

- SCCP: Configuring Multi-Party Ad Hoc and Meet-Me Conferencing, page 675 (required)

Modifying 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

Restrictions

- 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: – Cisco 2600 series, Cisco 2801—8 – Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3600 series, Cisco 3700 series—16 – Cisco 3800 series—24 (requires Cisco IOS Release 12.3(11)XL or a higher release) – 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.

What to Do Next

- To configure optional end-of-conference options for three-party ad hoc conferencing on SCCP phones, see "SCCP: Configuring Conferencing Options on a Phone" section on page 671
- To configure optional end-of-conference options for three-party ad hoc conferencing on SCCP phones, see "SIP: Configuring Conferencing Options on a Phone" section on page 673

SCCP: Configuring Conferencing Options on a Phone

To configure optional end-of-conference options for three-party ad hoc conferencing on a Cisco Unified IP phone running SCCP, perform the following steps for each phone to be configured.

Prerequisites

- 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 "Configuring Call Transfer and Forwarding" on page 517.

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.

	Command or Action	Purpose
Step 3	**`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 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. **Note** Analog phones connected to the Cisco Unified CME system through a Cisco VG 224 require Cisco IOS Release 12.3(11)YL1 or a later release to use this feature. • **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 "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

SIP: Configuring Conferencing Options on a Phone

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.

Prerequisites

- To facilitate call transfer by using the Confrn softkey, conference and transfer attended or transfer blind must be enabled. For configuration information, see "Configuring Call Transfer and Forwarding" on page 517.

Restrictions

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool pool-tag**
4. **keep-conference**
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. • *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.

	Command or Action	Purpose
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. • 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.
Step 5	**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 "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

Verifying Three-Party Ad Hoc Conferencing

Step 1 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.

```
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

Step 1 Use the **debug ephone** commands to observe messages and states associated with an ephone. For more information, see the *Cisco Unified CME Command Reference*.

SCCP: Configuring Multi-Party Ad Hoc and Meet-Me Conferencing

To configure multi-party ad hoc conference support for 3-8 parties plus Meet-Me conferencing for up to 32 parties, perform the following tasks:

- SCCP: Configuring Join and Leave Tones, page 676 (optional)
- SCCP: Configuring SCCP for Cisco Unified CME, page 678 (required)
- SCCP: Configuring the DSP Farm, page 679 (required)
- SCCP: Associating Cisco Unified CME with a DSP Farm Profile, page 681 (required)
- SCCP: Enabling Multi-Party Ad Hoc and Meet-Me Conferencing, page 682 (required)
- SCCP: Configuring Multi-Party Ad Hoc Conferencing and Meet-Me Numbers, page 683 (required)
- SCCP: Configuring Conferencing Options for a Phone, page 685 (required)
- SCCP: Verifying Multi-Party Ad Hoc and Meet-Me Conferencing, page 688 (optional)

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

Restrictions

- 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.
- Ad hoc conferencing for more than three parties (hardware-based) is not supported on the Cisco Unified IP Phone 7906 and 7910 and Cisco Unified IP Phone 7914 Expansion Module.
- Ad hoc conferencing for more than three parties is not supported on Cisco Unified IP phones running SIP.
- Hardware-based ad hoc conferencing does not support the local-consult transfer method (**transfer-system local-consult** command).

SCCP: Enabling 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.

SCCP: Configuring Join and Leave Tones

To configure tones to be played when parties join and leave ad hoc 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.
Step 7	**end** **Example:** `Router(cfg-cp-dualtone)# exit`	Exits configuration mode and enters privileged EXEC mode.

SCCP: Configuring SCCP for Cisco Unified CME

To enable Skinny Client Control Protocol (SCCP) on Cisco Unified CME, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number* [**port** *port-number*]
4. **sccp ccm** {**ip-address** | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**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-type interface-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.
Step 4	**sccp ccm** {**ip-address** | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] **Example:** `Router(config)# sccp ccm 1.4.158.3 identifier 100 version 4.0`	Adds a Cisco Unified CME router to the list of available servers and set various parameters—including IP address or Domain Name System (DNS) name, port number, and version number. • *version-number*—Must be 4.0 or later.
Step 5	**sccp ccm group** *group-number* **Example:** `Router(config)# sccp ccm group 123`	Creates a Cisco Unified CME group.

	Command or Action	Purpose
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.

SCCP: Configuring the DSP Farm

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-party** *max-parties*
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	**dspfadrm 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 the "SCCP: Enabling DSP Farm Services for a Voice Card" section on page 676.
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 the "SCCP: Enabling DSP Farm Services for a Voice Card" section on page 676.
Step 7	**maximum conference-party** *max-parties* **Example:** `Router(config-dspfarm-profile)# maximum conference-party 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.

	Command or Action	Purpose
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.

SCCP: Associating Cisco Unified CME with a DSP Farm Profile

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.

	Command or Action	Purpose
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.

SCCP: Enabling Multi-Party Ad Hoc and Meet-Me Conferencing

To allow 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 ad hoc conferencing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **conference hardware**
5. **sdspfarm units** *number*
6. **sdspfarm tag** *number device-name*
7. **sdspfarm conference mute-on** *mute-on-digits* **mute-off** *mute-off-digits*
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	**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	**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.
Step 6	**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 "SCCP: Associating Cisco Unified CME with a DSP Farm Profile" section on page 681.
Step 7	**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 8	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

SCCP: Configuring Multi-Party Ad Hoc Conferencing and Meet-Me Numbers

To configure numbers for 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. **conference** {**ad-hoc** | **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 for the purposes of creating and configuring an extension (ephone-dn) for a Cisco Unified IP 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**]] **Example:** `Router(config-ephone-dn)# number 6789`	Associates a telephone or extension number with an ephone-dn in a Cisco Unified CME system. • Each DN for a conference must have the same primary and secondary number.

	Command or Action	Purpose
Step 5	**conference ad-hoc** or **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.

SCCP: Configuring Conferencing Options for a Phone

To configure a template of conferencing features such as the add party mode, drop party mode, and soft keys, for 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.

Restrictions

- 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.

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**] [**Park**] [**RmLstC**] [**Select**] [**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.
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 and meet-me 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.

	Command or Action	Purpose
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**] [**Park**] [**RmLstC**] [**Select**] [**Trnsfer**] **Example:** `Router(config-ephone-template)# softkeys connected Hold Trnsfer Park Endcall Confrn ConfList Join Select RmLstC`	Configures an ephone template for soft-key display during the connected call stage. • The soft keys added are **RmLstC**, **ConfList**, **Join**, and **Select**. • 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**] **Example:** `Router(config-ephone-template)# softkeys hold Join Newcall Resume Select`	Configures an ephone template to modify soft-key display during the call-hold call stage. • The soft keys added are **Join** and **Select**. • 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 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 soft-key display during the idle call stage. • The soft keys added for multi-party conferencing are **RmLstC**, **ConfList**, and **Join**. • 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 soft-key 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 Ethernet phone (ephone) configuration mode for an IP phone for the purposes of creating and configuring an ephone.

	Command or Action	Purpose
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 "SCCP: Generating Configuration Files for SCCP Phones" on page 267.

SCCP: Verifying Multi-Party Ad Hoc and Meet-Me Conferencing

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.

show ephone-dn conference: Example

```
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
```

show telephony-service conference hardware detail: Example

```
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
```

Configuration Examples for Conferencing

This section provides the following configuration examples:

Basic Conferencing: Example

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
```

End of Conference Options: Example

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.

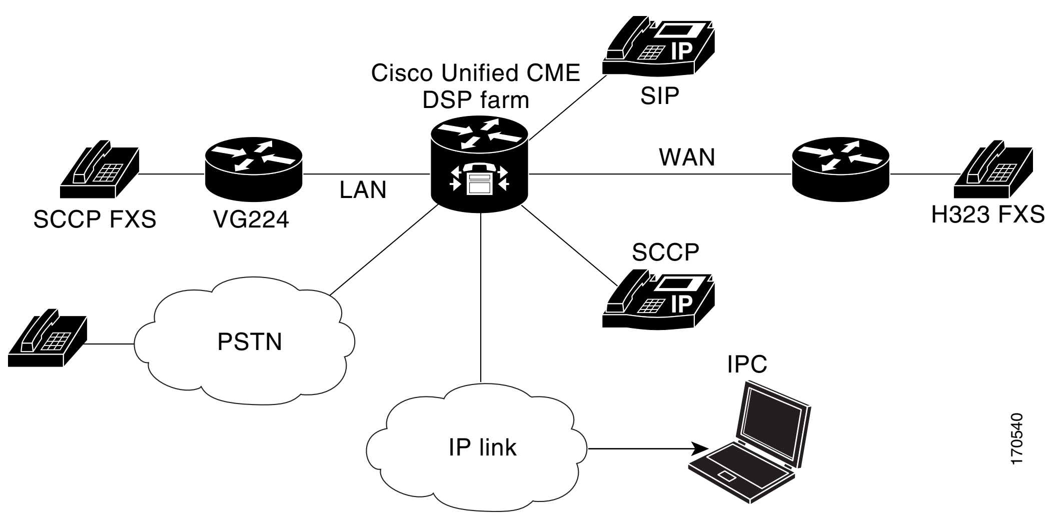
```
ephone-dn 39
 number 3999

ephone 29
 button 1:39
 keep-conference endcall local-only
```

DSP Farm and Cisco Unified CME on the Same Router: Example

In this example, the DSP farm and Cisco Unified CME are on the same router as shown in Figure 43.

Figure 43 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
!
```

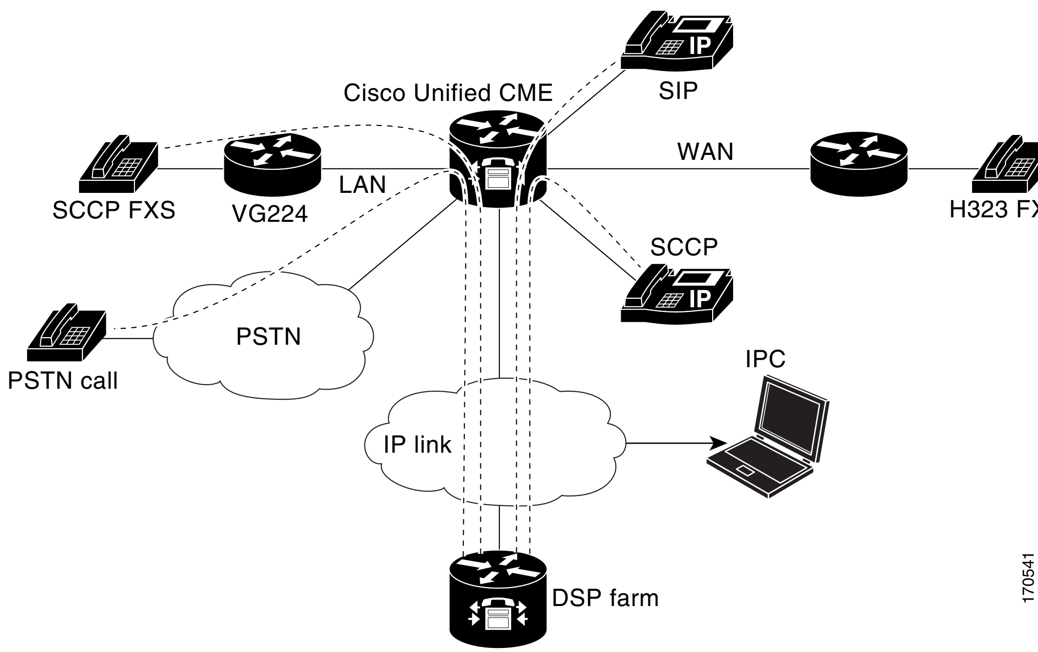
```
!
ephone-dn 3 dual-line
 number 8003
!
!
ephone-dn 4 dual-line
 number 8004
!
!
ephone-dn 5 dual-line
 number 8005
!
!
ephone-dn 6 dual-line
 number 8006
!
!
ephone-dn 7 dual-line
 number 8007
!
!
ephone-dn 8 dual-line
 number 8008
!
!
ephone-dn 60 dual-line
 number 8887
 conference meetme
 no huntstop
!
!
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
```

DSP Farm and Cisco Unified CME on Different Routers: Example

In this example, the DSP farm and Cisco Unified CME are on different routers as shown in Figure 44.

Figure 44 Cisco Unified CME and the DSP Farm on Different Routers



This section contains configuration examples for the following routers:

- Cisco Unified CME Router Configuration: Example, page 695
- DSP Farm Router Configuration: Example, page 702

Cisco Unified CME Router Configuration: Example

```
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
```

DSP Farm Router Configuration: Example

```
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 "Creating Templates" on page 927.

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 "Customizing Soft Keys" on page 875.

Additional References

The following sections provide references related to conferencing.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	• *Cisco Unified CME Command Reference* • *Cisco Unified CME Documentation Roadmap*
Cisco IOS voice configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Conferencing

Table 36 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 36 lists the 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.

Table 36 Feature Information for Conferencing

Feature Name	Cisco Unified CME Version	Feature Information
Meet-me Conferences	4.1	Added support for hardware-based meet-me conferences created by parties calling a designated conference number.
Multi-party Ad Hoc Conferencing	4.1	Added support for hardware-based Multi-party Conferencing Enhancements which uses digital signal processors (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 Conferencing	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.

Configuring Directory Services

Last Updated: March 26, 2007

This chapter describes the directory services support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Directory Services" section on page 725.

Contents

Information About Directory Services

To enable directory services, you should understand the following concepts:

- Local Directory, page 708
- External Directory, page 708
- Called-Name Display, page 708

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 Cisco 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 can display with first names first or last names first.

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 the "Configuring Local Directory Service" section on page 709.

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 several 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. For example, 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?" The called-name display feature 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.

How to Configure Directory Services

This section contains the following tasks:

Configuring 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.

	Command or Action	Purpose
Step 4	**directory** {**first-name-first** | **last-name-first**} **Example:** `Router(config-telephony)# directory last-name-first`	Defines the format for entries in the local directory. • 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.

SCCP: Defining a Name for a Directory Number

To define a name for a directory number in a local directory, perform the following steps.

Prerequisites

- 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 "SCCP: Creating Directory Numbers" on page 177.

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`	Associates a name with this directory number. 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 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Adding an Entry to a Local Directory

To add an entry to the local directory, perform the following steps.

Restrictions

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **directory entry** {*entry-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** {*entry-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. • *entry-tag*—Unique sequence number that identifies this directory entry during all configuration tasks. Range is 1 to 100. • If this name is to be used for called-name display, the *number* associated with the names must contain at least one wildcard character.
Step 5	**end** **Example:** `Router(config-telephony)# end`	Returns to privileged EXEC mode.

SCCP: Configuring External Directory 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.

Prerequisites

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.

Restrictions

Provisioning of 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** {**directory** | **service**} *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`** `{`**`directory`** `|` **`service`**`}` *`url`* **Example:** `Router(config-telephony)# url directory http://10.0.0.11/localdirectory`	Associates a URL with the programmable Directories and Services feature buttons 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-telephony)# end`	Exits configuration mode and enters privileged EXEC mode.

SCCP: Enabling Called-Name Display

To enable called-name display, perform the following steps.

Prerequisites

- 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 the "SCCP: Adding an Entry to a Local Directory" section on page 711.
- 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 the "SCCP: Defining a Name for a Directory Number" section on page 710

Restrictions

- The **service dnis overlay** command can only be used to configure overlaid ephone-dns.

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.

	Command or Action	Purpose
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.

Verifying 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.

```
Router# show running-config

telephony-service
 service dnis overlay
```

Step 2 Use the **show telephony-service directory-entry command** to display current directory entries.

```
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.

```
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.

```
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
```

SIP: Defining a Name for a Directory Number

To define name for a directory number on a SIP phone, perform the following steps.

Prerequisites

- 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 "SIP: Creating Directory Numbers" on page 181.

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.

	Command or Action	Purpose
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 **Example:** `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.
Step 5	**end** **Example:** `Router(config-register-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

SIP: Configuring External Directory 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.

Prerequisites

Cisco CME 3.4 or a later version.

Restrictions

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register global**
4. **url** {**directory** | **service**} *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	**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** | **service**} *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`	Associates a URL with the programmable Directories and Services feature buttons 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 configuration mode and enters privileged EXEC mode.

Verifying Directory Services

To verify the configuration for local directory services, perform the following steps.

SUMMARY STEPS

1. **show running-config**
2. **show telephony-service**
3. **show telephony-service directory-entry**

DETAILED 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.

```
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

This section contains the following examples:

- Local Directory, page 719
- Called-Name Display, page 720

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
```

The following example disables the local directory on IP phones served by the Cisco Unified CME router:

```
telephony-service
 no service local-directory
```

Called-Name Display

This section contains the following examples:

- First Ephone-dn in the Overlay Set: Example, page 720
- Directory Name for an Overlaid Ephone-dn Set: Example, page 720
- Directory Name for a Hunt Group with Overlaid Ephone-dns: Example, page 721
- Directory Name for Non-Overlaid Ephone-dns: Example, page 722
- Ephone-dn Name for Overlaid Ephone-dns: Example, page 723

First Ephone-dn in the Overlay Set: Example

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).

Directory Name for an Overlaid Ephone-dn Set: Example

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 the "Local Directory" section on page 708. For more information about overlaid ephone-dns, see "Configuring Call-Coverage Features" on page 581.

Directory Name for a Hunt Group with Overlaid Ephone-dns: Example

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 number 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 "Configuring Call-Coverage Features" on page 581. Note that wildcards are used only in secondary numbers and cannot be used with primary numbers. For more information about making directory entries, see the "Local Directory" section on page 708. For more information about overlaid ephone-dns, see "Configuring Call-Coverage Features" on page 581.

Directory Name for Non-Overlaid Ephone-dns: Example

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 the "Local Directory" section on page 708.

Ephone-dn Name for Overlaid Ephone-dns: Example

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 "Configuring Call-Coverage Features" on page 581.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Directory Services

Table 37 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 37 lists the 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.

Table 37 Feature Information for Directory Services

Feature Name	Cisco Unified CME Version	Feature Information
Called-Name Display	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.

Configuring Do Not Disturb

Last Updated: March 26, 2007

This chapter describes the do-not-disturb feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Do Not Disturb" section on page 734.

Contents

Information About Do Not Disturb

To configure do not disturb, you should understand the following concept:

- Do Not Disturb, page 727

Do Not Disturb

The Do Not Disturb (DND) feature allows you to set your phone to forward calls without ringing the phone. Enable DND service using the DND soft key on Cisco Unified IP phones that support soft keys. When DND is enabled, incoming calls do not ring on the phone, but they do provide visual alerting and call information and 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" is displayed on the calling phone indicating that the target phone is in the DND state.

Pressing the DND soft key during an incoming call forwards the call to the call-forward destination if call-forward is enabled. If call-forward is not enabled, pressing the DND soft key disables the ringer and visual alerting.

You can use the DND soft key to switch on or off the DND functionality in all call states except connected. That is, you can enable or disable DND when an incoming call is ringing or when you are not connected to a call. You cannot enable or disable DND when you are connected to an incoming call.

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.

How to Configure Do Not Disturb

This section contains the following tasks:

- SCCP: Blocking Do Not Disturb, page 728 (required)
- SCCP: Verifying Do Not Disturb, page 729 (optional)
- SIP: Configuring Do Not Disturb, page 730 (required)

SCCP: Blocking Do Not Disturb

To block DND on phones that have buttons configured for feature ringing, perform the following steps. DND is enabled by using the DND soft key on Cisco Unified IP phones that support soft keys.

Prerequisites

- Cisco Unified 3.2.1 or a later version.
- Call-forwarding no-answer must be set for a phone to use DND to forward calls. For configuration information, see "Configuring Call Transfer and Forwarding" on page 517. No other configuration is necessary for basic DND.

Restrictions

- Phone users cannot enable DND for a shared line in a hunt group. The soft key displays in the idle and ringing states but does not enable DND for shared lines in hunt groups.

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* **Example:** `Router(config)# ephone 10`	Enters ephone configuration mode. • *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`	Allows phone buttons configured with the feature-ring option to ring when their IP phones are in do-not-disturb (DND) mode.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

SCCP: Verifying Do Not Disturb

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
```

SIP: Configuring Do Not Disturb

To configure the Do-not-Disturb (DND) feature on a SIP phone with softkeys, perform the following steps.

Note You can enable the Do-Not-Disturb (DND) soft key on one or more SIP phones by using the **dnd-control** command in voice register template configuration mode. For information about configuring templates, see "Creating Templates" on page 927.

Prerequisites

- Cisco CME 3.4 or a later version.
- Call-forwarding busy must be set for a SIP IP phone to use DND to forward calls. For configuration information, see "Configuring Call Transfer and Forwarding" on page 517.

Restrictions

- If the DND soft key is disabled by a user on the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, or 7971GE, it does not display after the phone is reset or restarted. DND must be enabled both in Cisco Unified CME *and* by using the DND soft key on the phone.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-tag*
4. **dnd**
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 to set parameters for SIP phone to be configured.

	Command or Action	Purpose
Step 4	**dnd** **Example:** `Router(config-register-pool)# dnd-control`	Enables DND. **Note** If call-forward-no-answer is not configured for the extension, pressing the DND key mutes the ringer until the caller terminates the call.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuration Examples for Do Not Disturb

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
```

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 soft key, they do not receive calls on any extension on their phones. When they use the HLog soft key, 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 "Configuring Call-Coverage Features" on page 581.

Call Forwarding

To use the DND soft key to forward calls, enable call-forwarding no-answer for SCCP phones or call-forward busy for SIP IP phones. See "Configuring Call Transfer and Forwarding" on page 517.

Feature Access Codes (FACs)

DND can be activated and deactivated using a feature access code (FAC) instead of the DND soft key when standard or custom FACs are enabled. The following is the standard FAC for DND:

- DND—**7

See "Configuring Feature Access Codes" on page 775.

Soft-Key Display

You can remove or change the position of the DND soft key. See "Customizing Soft Keys" on page 875.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Do Not Disturb

Table 38 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 38 lists the 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.

Table 38 Feature Information for Do Not Disturb

Feature Name	Cisco Unified CME Version	Feature Information
Do Not Disturb	3.4	Added support for Do-not-disturb (DND) soft key on supported Cisco Unified IP phones that are connected to a Cisco Unified CME router and running SIP.
	3.2.1	DND bypass for feature-ring phones was introduced.
	3.2	DND was introduced.

Configuring Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode

First Published: August 15, 2007

This chapter describes the Enhanced 911 Services feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode" section on page 762.

Contents

Prerequisites for Enhanced 911 Services

- Cisco IOS Release 12.4(15)T or a later release.
- Cisco Unified CME 4.1 or a later version, configured in SRST fallback mode. See "Configuring SRST Fallback Support" on page 989.
- 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 can use FXS, FXO, SIP, or H.323 trunk interfaces.

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 the "Precautions for Mobile Phones" section on page 740.
- The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL). For more information, see the "Overview of Enhanced 911 Services" section on page 737.
- 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 the "Multiple Usages of an ELIN" section on page 743.
- 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 the "Interactions with Existing Cisco Unified CME Features" section on page 742.

Information About Enhanced 911 Services

To configure Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode, you should understand the following concepts:

Note For information about configuring ephones, ephone-dns, voice register pools, and voice register dns, see "Configuring Phones to Make Basic Calls" on page 165.

Overview of Enhanced 911 Services

Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode enables 911 operators to:

- Immediately pinpoint the location of the 911 caller based on the calling number
- Callback the 911 caller if a disconnect occurs

Before this feature was introduced, Cisco Unified 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 would then have to verbally gather the emergency information and location from the caller, before dispatching a response team from the ambulance service, fire department, or police department. Calls could not be routed to different PSAPs, based on the specific geographic areas that they cover.

With Enhanced 911 Services, 911 calls are selectively routed to the closest PSAP based on the caller's location. In addition, the caller's phone number and address automatically display on a terminal at the PSAP. Therefore, the PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

To use Enhanced 911 Services, you must define an emergency response location (ERL) for each of the geographic areas needed to cover all of the phones supported by Cisco Unified 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.

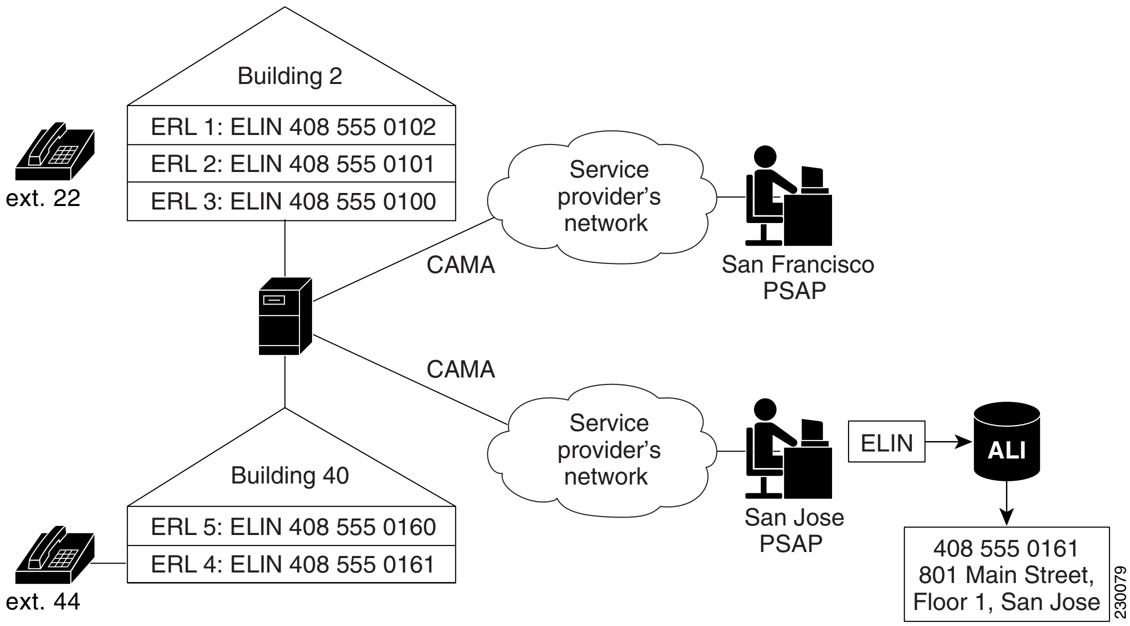
To determine which ERL is assigned to a 911 caller, the PSAP uses the caller's unique phone number, which is also known as the emergency location identification number (ELIN). Before you can use Enhanced 911 Services you must supply the PSAP with a list of your ELINs and street addresses for each ERL. 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 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 time limit of three hours.

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.

Figure 45 shows a multiline phone system handling phones 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.

Figure 45 Implementation of Enhanced 911 for Cisco Unified CME in SRST Mode



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.

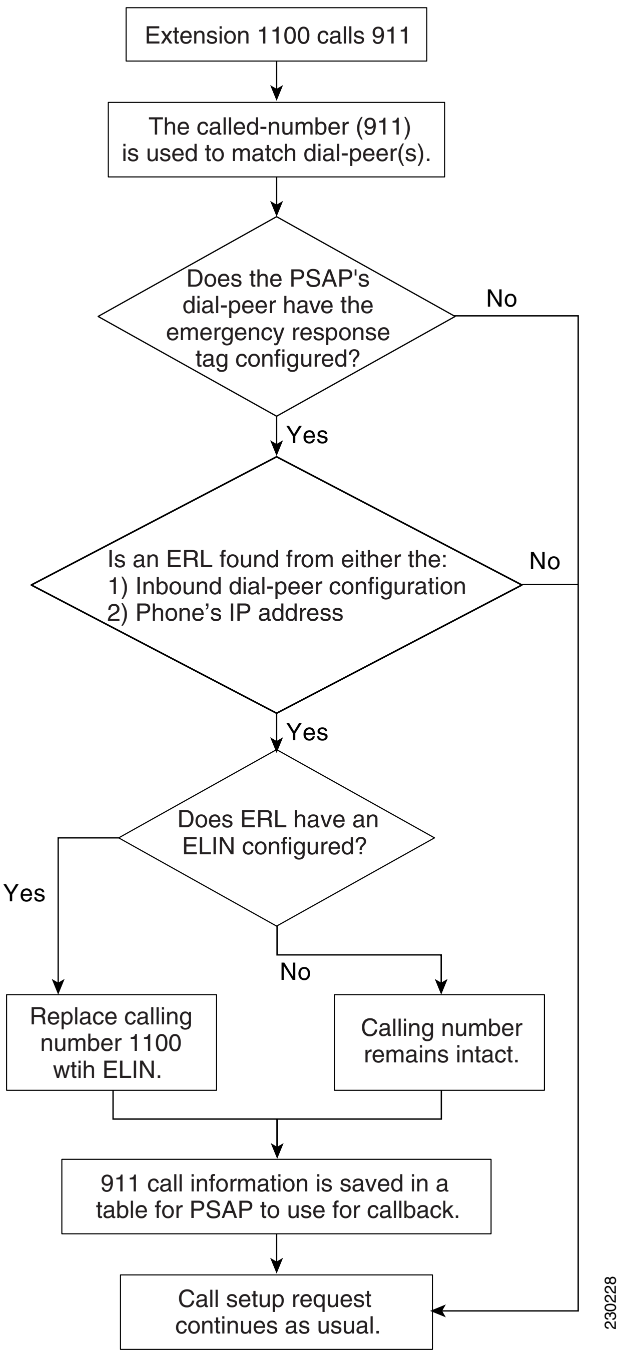
After an ELIN is determined for the call, the following information is saved to the Last Caller table:

- 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 three hours have passed after the call was originated. After the 911 call information is saved to the Last Caller table, 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 46 summarizes the procedure for processing a 911 call.

Figure 46 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 three hours have 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 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.

Planning Your Implementation of Enhanced 911 Services

Before you configure Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode:

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 39 shows an example of the information that you need to gather.

Table 39 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 40 shows an example.

Table 40 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 Optionally 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 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 5 Configure one or more dial peers for the PSAP's 911 callbacks with the **emergency response callback** command.

Step 6 Decide what method to use to assign the phones to each ERL.

You have the following choices:

- For a group of phones that are on the same subnet, you can create an IP subnet in the ERL that includes each phone's IP address. Each ERL can have one or two unique IP subnets. This is the easiest option to configure. Table 41 shows an example.

Table 41 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

Table 41 Definitions of ERL, Description, IP Subnets, and ELIN

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

- You can assign an ERL to a phone individually. Depending on which type of phone you have, you can use one of three methods. You can assign an ERL to a phone's:
  - Ephone configuration
  - Dial-peer configuration
  - Voice register pool configuration

  Table 42 shows examples of each of these options.

Table 42 Explicit ERL Assignment Per Phone

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

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

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

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

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

Call Forward

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

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

Call Blocking Features

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

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

Call Waiting

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

Three-Way Conference

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

Dial-Peer Rotary

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

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

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.

How to Configure Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode

How you configure Enhanced 911 Services depends on which decision you made in Step 6 in the "Planning Your Implementation of Enhanced 911 Services" section on page 741. However, there are three basic components that you must configure regardless of your planning decisions:

- An ERL with the ELIN, a PSTN number that will replace the caller's extension, as explained in the "Configuring the Emergency Response Location" section on page 746.
- A dial peer for emergency calls to the PSAP, as explained in the "Configuring a Dial Peer for Emergency Calls" section on page 747.
- A dial peer for callbacks from the PSAP, as explained in the "Configuring a Dial Peer for Callbacks from the PSAP" section on page 748.

In addition, you must specify an ERL for each phone. The type of phones that you have determines which of the following methods you will use to associate an ERL with your phones:

- If you choose 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. You define the groups of IP phones in terms of the IP subnets to which they belong, as explained in the "Assigning an ERL to a Phone's IP Subnet" section on page 750. You can optionally specify up to two different subnets.
- If you choose to assign an ERL to a phone's voice register pool, you must specify the ERL in the voice register pool configuration, as explained in the "Assigning an ERL to a SIP Phone" section on page 751.
- If you choose to assign an ERL to a phone's ephone, you must specify the ERL in the ephone configuration, as explained in the "Assigning an ERL to a Phone's Ephone" section on page 752.
- If you choose to assign an ERL to a phone's dial peer, you must specify the ERL in the dial-peer configuration, as explained in the "Assigning an ERL to a Dial Peer" section on page 753.

Configuring 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.

Prerequisites

Cisco Unified CME 4.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice emergency response location** *tag*
4. **elin** [**1** | **2**] *E.164-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 location`** *`tag`* **Example:** `Router(config)# voice emergency response location 4`	Enters emergency response location configuration mode to define parameters for an ERL.

	Command or Action	Purpose
Step 4	**elin** [**1** | **2**] *E.164-number* **Example:** `Router(cfg-emrgncy-resp-location)# elin 1 4085550100`	(Optional) Specifies the ELIN, an E.164 PSTN number that replaces the caller's extension. • This number is displayed on the PSAP's terminal and is used by the PSAP to query the ALI database to locate the caller. It is also used by the PSAP for callbacks. You can define a second ELIN using the optional **elin 2** command. If an ELIN is not defined for the ERL, the PSAP sees the original calling number.
Step 5	**end** **Example:** `Router(cfg-emrgncy-resp-location)# end`	Returns to privileged EXEC mode.

Configuring a Dial Peer 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.

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

Configuring a Dial Peer for Callbacks from the PSAP

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *number* **pots** **Example:** `Router(config)# dial-peer voice 100 pots`	Enters dial-peer configuration mode to define parameters for an individual dial peer.
Step 4	**incoming called-number** *number* **Example:** `Router(config-dial-peer)# incoming called-number 4085550100`	(Optional) Selects the inbound dial peer based on the called number to identify the last caller. This number is the ELIN.
Step 5	**direct-inward-dial** **Example:** `Router(config-dial-peer)# direct-inward-dial`	(Optional) Enables the Direct Inward Dialing (DID) call treatment for the incoming called number. For more information, see the 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.

Assigning an ERL to a Phone's IP Subnet

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice emergency response location** *tag* **Example:** `Router(config)# voice emergency response location 4`	Enters emergency response location configuration mode to define parameters for an ERL.
Step 4	**subnet** [**1** | **2**] *IPaddress-mask* **Example:** `Router(cfg-emrgncy-resp-location)# subnet 1 192.168.0.0 255.255.0.0`	Defines the groups of IP phones that are part of this location. You can create up to 2 different subnets. • To include all IP phones on a single ERL, use the **command subnet 1 0.0.0.0 0.0.0.0** to configure a default subnet. This subnet does not apply to nonIP-phone endpoints, such as phones on VoIP trunks or FXS/FXO trunks.
Step 5	**end** **Example:** `Router(cfg-emrgncy-resp-location)# end`	Returns to privileged EXEC mode.

Assigning an ERL to a 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 6 in the "Planning Your Implementation of Enhanced 911 Services" section on page 741.

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. The tag is an integer from 1 to 2147483647. If the ERL's tag is not a configured tag, the phone is not associated to an ERL and the phone defaults to its IP address to find the inclusive ERL subnet.
Step 5	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.

Assigning an ERL to a Phone's Ephone

Perform this procedure if you chose to assign an ERL to a phone's ephone instead of configuring an ERL to be associated with IP subnets. For more information about this decision, see Step 6 in the "Planning Your Implementation of Enhanced 911 Services" section on page 741.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ephone** *tag* **Example:** `Router(config)# ephone 224`	Enters ephone configuration mode to define parameters for an individual ephone.
Step 4	**emergency response location** *tag* **Example:** `Router(config-ephone)# emergency response location 12`	Assigns an ERL to a phone's ephone configuration using an ERL's tag. The tag is an integer from 1 to 2147483647. If the ERL's tag is not a configured tag, the phone is not associated to an ERL and the phone defaults to its IP address to find the inclusive ERL subnet.
Step 5	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Assigning an ERL to a Dial Peer

Perform this procedure to assign an ERL to a FXS/FXO or VoIP dial peer. Because these interfaces do not have IP addresses associated with them, you must use this procedure instead of configuring an ERL to be associated with IP subnets. For more information about this decision, see Step 6 in the "Planning Your Implementation of Enhanced 911 Services" section on page 741.

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.

Verifying Enhanced 911 Services

Step 1 Use the **show voice emergency callers** command to see the translations made by outbound 911 calls. This command lists the originating number, the ELIN used, and the time for each 911 call. This history is active for only three hours after the call is placed. Expired calls are not shown in this output.

```
router# show voice emergency callers

EMERGENCY CALLS CALL BACK TABLE
ELIN                      | CALLER                      | TIME
6045550100                | 6045550150                  | Oct 12 2006 03:59:43
6045550110                | 8155550124                  | Oct 12 2006 04:05:21
```

Troubleshooting Enhanced 911 Services

Step 1 Use the **debug voice application error** and the **debug voice application callsetup** command. These are existing commands for calls made using the default session or TCL applications.

This example shows the debug output when a call to 911 is made:

```
router# debug voice application error
router# debug voice application callsetup

Nov 10 23:49:05.855: //emrgncy_resp_xlate_callingNum: InDialPeer[20001], OutDialPeer[911]
callingNum[6046692003]
Nov 10 23:49:05.855: //ER_HistTbl_Find_CallHistory: 6046699100
Nov 10 23:49:05.855: //59//Dest:/DestProcessEmergencyCall: Emergency Call detected: Using
ELIN 6046699100
```

This example shows the debug output when a PSAP calls back an emergency caller:

```
router# debug voice application error
router# debug voice application callsetup

Nov 10 23:49:37.279: //emrgncy_resp_xlate_calledNum: calledNum[6046699100],
dpeerTag[6046699]
Nov 10 23:49:37.279: //ER_HistTbl_Find_CallHistory: 6046699100
Nov 10 23:49:37.279: //HasERHistoryExpired: elapsedTime[10 minutes]
Nov 10 23:49:37.279: //67//Dest:/DestProcessEmergencyCallback: Emergency Response
Callback: Forward to 6046692003.
Nov 10 23:49:37.279: //67//Dest:/DestCaptureCallForward: forwarded to 6046692003 reason 1
```

Error Messages

The Enhanced 911 feature introduces a new system error message. The following error message displays if a 911 callback cannot route to the last 911 caller because the saved history was lost because of a reboot, an expiration of an entry, or a software error:

```
%E911_NO_CALLER:  Unable to contact last 911 caller.
```

Configuration Examples for Enhanced 911 Services

This section contains the following example:

- Enhanced E911 Services with Cisco Unified CME in SRST Fallback Mode: Example, page 755

Enhanced E911 Services with Cisco Unified CME in SRST Fallback Mode: Example

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
```

Additional References

The following sections provide references related to Enhanced 911 Services for Cisco Unified CME in SRST fallback mode.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	• *Cisco Unified CME System Administrator Guide* • *Cisco Unified CME Command Reference*
Cisco IOS voice configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference* • *Cisco IOS Debug Command Reference* • *Cisco IOS Tcl IVR and VoiceXML Application Guide*
Phone documentation for Cisco Unified CME	• *User Guides and Quick Reference Cards*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Enhanced 911 Services for Cisco Unified CME in SRST Fallback Mode

Table 43 lists the enhancements to the Enhanced 911 Services feature by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 43 lists the 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.

Table 43 Feature Information for Enhanced 911 Services

Feature Name	Cisco Unified CME Version	Feature Information
Enhanced 911 Services	4.1	Enhanced 911 Services was introduced.

Configuring Extension Mobility

Last Updated: September 7, 2007
First Published: June 18, 2007

This module describes features in Cisco Unified Communications Manager Express (Cisco Unified CME) that provide support for phone mobility for end users.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Extension Mobility" section on page 774.

Contents

Information About Extension Mobility

To configure interoperability, you should understand the following concepts:

- Extension Mobility, page 763

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 button on the phone is configured with a login service URL hosted by Cisco Unified CME that points to the Extension Mobility Login page.

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 in a sequence. 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 the "How to Enable Extension Mobility" section on page 764.

How to Enable Extension Mobility

Perform the following tasks to enable Extension Mobility in Cisco Unified CME:

- Configuring a Logout Profile for an IP Phone, page 765 (required)
- Enabling an IP Phone for Extension Mobility, page 767 (required)
- Configuring a User Profile, page 769 (required)

Prerequisites

- Cisco Unified CME 4.2 or a later version.

Restrictions

- Extension Mobility on remote Cisco Unified CME routers is not supported; a phone user can log into any local Cisco Unified IP phone only.

Configuring 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.

Prerequisites

- 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 "Configuring Phones to Make Basic Calls" on page 165.

Restrictions

- For button appearance, Extension Mobility associates directory numbers, then speed-dial definitions in the logout profile or user profile to phone buttons in a sequence beginning with numbers, 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 will be downloaded to buttons.
- The first number to be configured for line appearance cannot be a monitored directory number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice logout-profile** *tag*
4. **user** *name* **password** *password*
5. **number** *number* **type** *type*
6. **speed-dial** *speed-tag number* [**label** *label*] [**blf**]
7. **pin** *pin*
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 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 a Cisco Unified CME. • *name*—Alphanumeric string. • *password*—Alphanumeric string.
Step 5	**number** *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** *pin* **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. • *pin*—Numeric string containing four to eight digits.
Step 8	**end** **Example:** `Router(config-logout-profile)# end`	Exits to privileged EXEC mode.

Enabling 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.

Prerequisites

- 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.

Restrictions

- Extension Mobility is not supported on Cisco Unified IP phones without phone screens.
- Extension Mobility is not supported for SIP IP phones.
- Extension Mobility is not supported for analog devices.

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.

	Command or Action	Purpose
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. • *mac-address*—MAC address of phone, which is found on a sticker located on the bottom of the phone.
Step 5	**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.
Step 6	**type** *phone-type* **Example:** `Router(config-ephone)# type 7960`	Defines a phone type for the phone being configured.
Step 7	**end** **Example:** `Router(config-ephone)# end`	Exits to privileged EXEC mode.

Configuring 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.

Prerequisites

- 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 "Configuring Phones to Make Basic Calls" on page 165.

Restrictions

- For button appearance, Extension Mobility associates directory numbers, then speed-dial definitions in the logout profile or user profile to phone buttons in a sequence beginning with numbers, 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 will be downloaded to buttons.
- The first number to be configured for line appearance cannot be a monitored directory number.

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** *pin*
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 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*—Name of authorized user. • *password*—Password for authorized user.
Step 5	**number** *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. • **blf**—(Optional) Enables Busy Lamp Field (BLF) monitoring for a speed-dial number.

	Command or Action	Purpose
Step 7	**pin** *pin* **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. • *pin*—Numeric string containing four to eight digits.
Step 8	**end** **Example:** `Router(config-user-profile)# end`	Exits to privileged EXEC mode.

Configuration Examples for Extension Mobility

This section contains the following configuration examples:

- Logout Profile: Example, page 771
- Enabling an IP Phone for Extension Mobility: Example, page 771
- Voice-User Profile: Example, page 772

Logout Profile: Example

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 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.

```
 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
```

Enabling an IP Phone for Extension Mobility: Example

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
```

User Profile: Example

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 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.

```
 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 "Resetting and Restarting Phones" on page 277.
- If you enabled one or more Cisco Unified IP phones for Extension Mobility, generate a new configuration file and restart the phones. See "Generating Configuration Files for Phones" on page 265.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Extension Mobility

Table 44 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified Communications Manager Express and Cisco IOS Software Version Compatibility Matrix* at
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 44 lists the 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.

Table 44 Feature Information for Extension Mobility

Feature Name	Cisco Unified CME Version	Modification
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.

Configuring Feature Access Codes

Last Updated: March 26, 2007

This chapter describes the feature access codes support in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Feature Access Codes" section on page 781.

Contents

Information About Feature Access Codes

To enable Feature Access Codes, you should understand the following concept:

- Feature Access Codes, page 776

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 phones users select soft keys 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 Trnsfer soft key (IP phones) or hookflash (analog phones) is used to initiate a transfer.

Table 45 contains a list of the standard predefined FACs.

Table 45 Standard FACs

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 soft key (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 an hunt group agent is off-hook.

Table 45 Standard FACs (continued)

Standard FAC	Description
*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.
#3	Leave ephone-hunt group. Telephone or extension number must already be configured as a dynamic member of a hunt group.

How to Configure Feature Access Codes

This section contains the following tasks:

- Enabling Feature Access Codes, page 777
- Verifying Feature Access Codes, page 778

Enabling 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.

	Command or Action	Purpose
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. • *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.

Verifying Feature Access Codes

To verify the FAC configuration, perform the following step.

Step 1 **show telephony-service fac**

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
```

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

This section contains the following configuration example:

- FAC: Example, page 779

FAC: Example

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 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 add s the 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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Feature Access Codes

Table 46 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 46 lists the 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.

Table 46 Feature Information for Feature Access Codes

Feature Name	Cisco Unified CME Version	Feature Information
Feature Access Codes	4.0	Feature access codes (FACs) were introduced.

Configuring Fax Relay

First Published: June 18, 2007

This module 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.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Fax Relay" section on page 790.

Contents

Prerequisites for Fax Relay

- Cisco Unified CME 4.0(3) or a later version.
- Cisco IOS Release 12.4(11)T or a later release.
- SCCP Telephony Control (STC) application is enabled.

Note If your voice gateway is a separate router than the Cisco Unified CME router, it must use an IP voice image of Cisco IOS Release 12.4(11)T or later.

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 VG 224, FXS port, or analog telephone adaptor (ATA) to use H.323 or Session Initiation Protocol (SIP) with a specific fax relay protocol. See the *Cisco IOS Fax and Modem Services over IP Application Guide.*
- G.711 Fax Pass-Through with SCCP
  - This is the default setup for facsimile on Cisco VG 224 and FXS ports before Cisco Unified CME 4.0(3). See the *Cisco IOS Fax and Modem Services over IP Application 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 47, Supported Gateways, Modules, and VICs for Fax Relay.

Information About Fax Relay

To configure the fax relay feature, you should understand the following:

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 VG 224).
- The fax relay feature facilitates replacement of the PSTN time-division multiplexing (TDM) infrastructure with VoIP.

Feature Design of Cisco Fax Relay

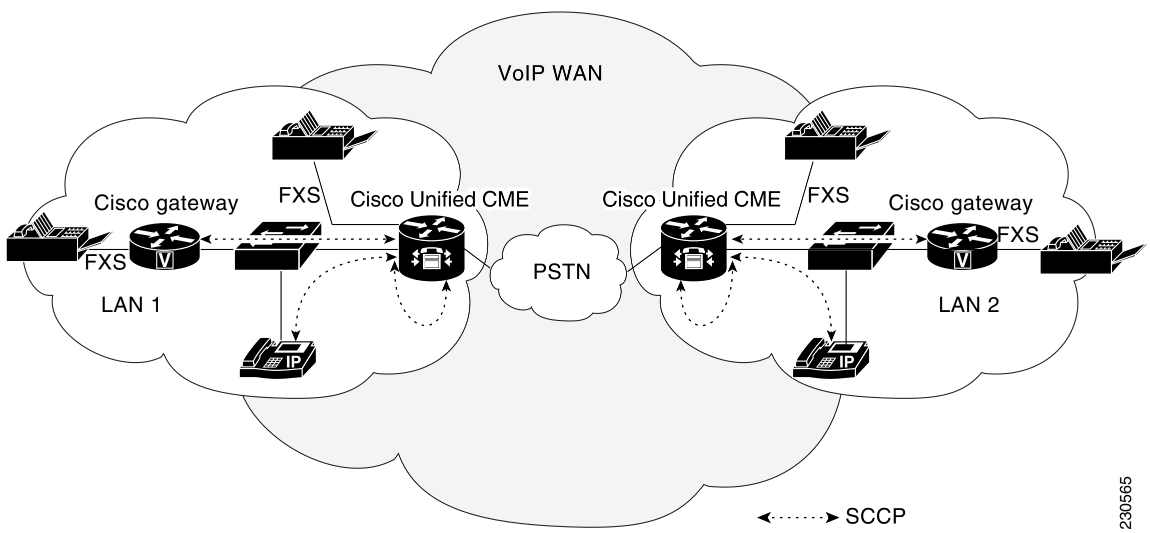
Cisco Fax Relay is a proprietary fax relay implementation that uses Real-time Transport Protocol (RTP) to transport fax data. It is the default fax relay type on Cisco voice gateways. The fax relay feature provides enhanced supplementary feature capability on analog ports connected to a Cisco integrated services router (ISR) or Cisco VG 224 analog gateway. Calls through the analog FXS ports are controlled by a 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 47 shows a multisite deployment of the fax relay feature in a Cisco Unified CME topology.

Figure 47 Cisco Unified CME Fax Relay Deployment



For information on configuring gateway-controlled fax relay features, see the "How to Configure Fax Relay" section on page 786.

Supported Gateways, Modules, and Voice Interface Cards for Fax Relay

Table 47 lists supported gateways, modules, and voice interface cards (VICs).

Table 47 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	—	—	—

How to Configure Fax Relay

This section contains the following tasks:

- Configuring Fax Relay, page 786 (required)
- Verifying and Troubleshooting Fax Relay Configuration, page 788 (optional)

Configuring Fax Relay

To configure the fax relay features on Cisco Unified CME, perform the following steps.

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.
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.
Step 6	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits the current configuration mode.

Troubleshooting Tips

The following commands can help troubleshoot SCCP fax relay features:

- **debug voip application stcapp all**
- **debug voip vtsp all**

Note For more information on these and other commands, see the *Cisco IOS Voice Command Reference*, *Cisco IOS Debug Command Reference,* Release 12.4T, *Cisco Unified Communications Manager Express Command Reference*, and *Cisco IOS Configuration Fundamentals Command Reference,* Release 12.4.

Verifying and Troubleshooting Fax Relay Configuration

To verify the configuration of Cisco Fax Relay, use the **show-running config** command. Sample output is located in the "Configuration Examples for Fax Relay" section on page 788.

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 the *Cisco IOS Voice Command Reference*, *Cisco IOS Debug Command Reference,* Release 12.4T, *Cisco Unified Communications Manager Express Command Reference*, and *Cisco IOS Configuration Fundamentals Command Reference,* Release 12.4.

Configuration Examples for Fax Relay

This section contains the following example:

- Fax Relay: Example, page 788

Fax Relay: Example

```
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
```

Additional References

The following sections provide references related to Cisco Fax Relay.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	*Cisco Unified Communications Manager Express System Administrator Guide*
Cisco Unified CME command reference	*Cisco Unified Communications Manager Express Command Reference*
Cisco IOS debugging	*Cisco IOS Debug Command Reference,* Release 12.4T
Cisco IOS voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Fax and modem transmission on Cisco Voice over IP (VoIP) networks	*Cisco IOS Fax and Modem Service over IP Application Guide*
SCCP gateway controlled feature mode call control	*Feature Mode for SCCP FXS Ports in Cisco IOS*
SCCP gateway controlled VMWI	*VMWI for SCCP FXS Ports in Cisco IOS*
SCCP gateway controlled supplementary features	*SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways*
Platform-specific documentation for the following: • Cisco 2800 Series Integrated Services Routers • Cisco 3800 Series Integrated Services Routers • Cisco VG 224 Voice Gateway Router	http://www.cisco.com/en/US/products/hw/routers/index.html http://www.cisco.com/en/US/products/sw/voicesw/index.html

Technical Assistance

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

Feature Information for Fax Relay

Table 48 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 48 lists the 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.

Table 48 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 a Cisco Unified CME system.

Configuring Headset Auto-Answer

Last Updated: March 26, 2007

This chapter describes the headset auto-answer feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Headset Auto-Answer" section on page 797.

Contents

Information About Headset Auto-Answer

To enable the Headset Auto-Answer feature, you should understand the following concepts:

- Auto-Answering Calls Using a Headset, page 792
- Difference Between a Line and a Button, page 792

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

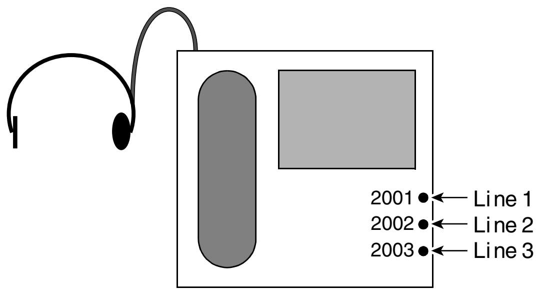
Note that a line is similar to, but not exactly the same as, a button on the phone. A line represents a phone's capability to make a call connection, so each button that can make a call connection becomes a line. (For example, unoccupied buttons or speed-dial buttons are not lines.) Note also that a 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 48 illustrates a comparison of line numbers and button numbers for different types of ephone configurations.

Figure 48 When is a Line the Same as a Button?

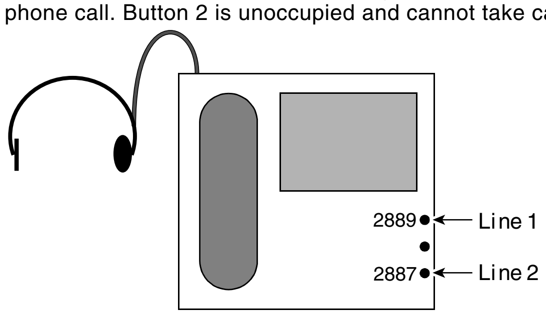
Most of the time, a line number is the same as the button number on which it appears.

In this example, line 1 is button 1, line 2 is button 2, and line 3 is button 3.



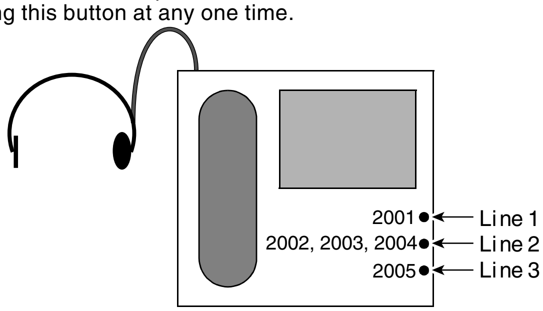

```
ephone-dn 21
 number 2001
ephone-dn 22
 number 2002
ephone-dn 23
 number 2003
ephone 2
 button 1:21 2:22 3:23
 headset auto-answer line 1
 headset auto-answer line 2
```

But not always. In the following case, line 2 is button 3, because button3 is the second button that has an ephone-dn to be connected to a phone call. Button 2 is unoccupied and cannot take calls.



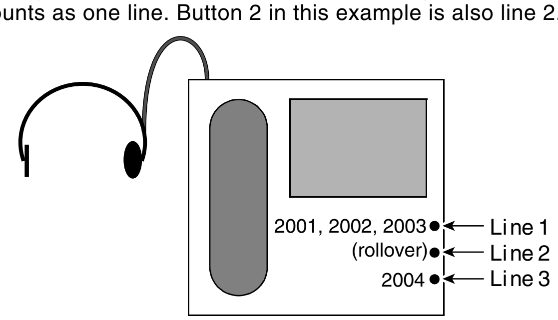

```
ephone-dn 33
 number 2889
ephone-dn 34
 number 2887
ephone 2
 button 1:33 3:34
 headset auto-answer line 1
 headset auto-answer line 2
```

In the following example, button 2 has three overlay ephone-dns (22, 23, and 24). Button 2 is defined as one line because only one of those ephone-dns can be connected to a call using this button at any one time.




```
ephone-dn 21
 number 2001
ephone-dn 22
 number 2002
ephone-dn 23
 number 2003
ephone-dn 24
 number 2004
ephone-dn 25
 number 2005
ephone 2
 button 1:21 2o22,23,24 3:25
 headset auto-answer line 2
 headset auto-answer line 3
```

An expansion, or rollover, line for overlaid ephone-dns also counts as one line. Button 2 in this example is also line 2.




```
ephone-dn 21
 number 2001
ephone-dn 22
 number 2002
ephone-dn 23
 number 2003
ephone-dn 24
 number 2004
ephone 2
 button 1o21,22,23 2x1 3:24
 headset auto-answer line 1
 headset auto-answer line 2
```

135076

How to Configure Headset Auto-Answer

This section contains the following tasks:

- Enabling Headset Auto-Answer, page 794 (required)
- Verifying Headset Auto-Answer, page 795 (optional)

Enabling Headset Auto-Answer

To enable headset auto-answer, perform the following steps.

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.

Verifying 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 Examples for 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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Headset Auto-Answer

Table 49 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 49 lists the 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.

Table 49 Feature Information for Headset Auto-Answer

Feature Name	Cisco Unified CME Version	Feature Information
Headset Auto-Answer	4.0	Headset auto-answer was introduced.

Configuring Intercom Lines

Last Updated: September 10, 2007

This chapter describes the intercom features in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Intercom Lines" section on page 807.

Contents

Information About Intercom Lines

To enable intercom lines, you should understand the following concept:

- Intercom Auto-Answer Lines, page 799

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 speakerphone mode with mute activated, which provides 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.

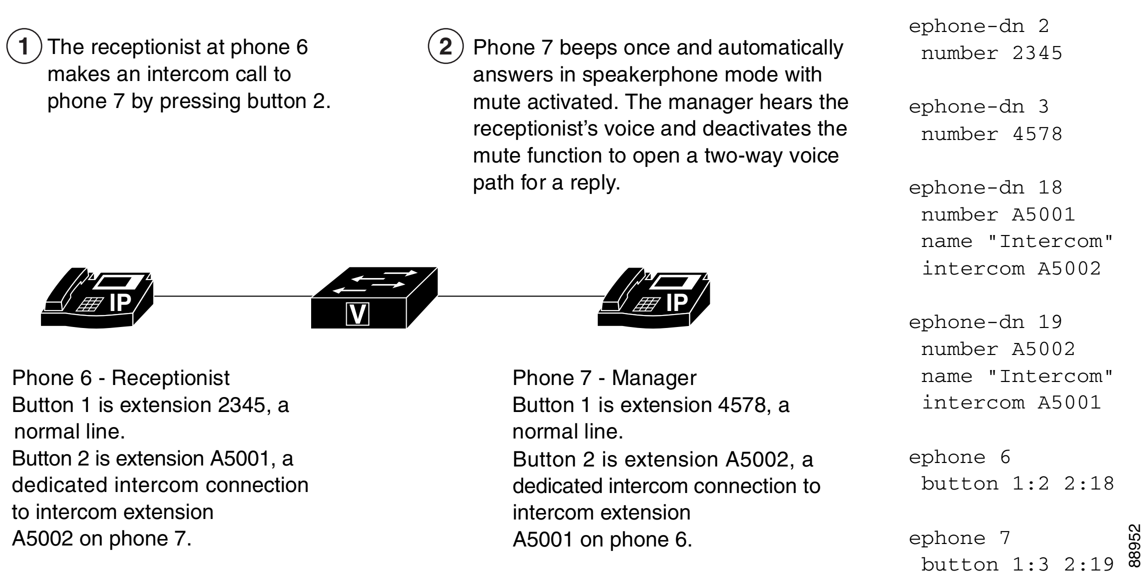
In Cisco CME 3.2.1 and later versions, you can deactivate the speaker-mute function on intercom calls. For example, if phone user 1 makes an intercom call to phone user 2, both users hear each other on connection when no-mute is configured. The benefit is that people who receive intercom calls can be 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 49 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 49 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 49 Intercom Lines



How to Configure Intercom Lines

This section contains the following tasks:

- SCCP: Configuring an Intercom Auto-Answer Line, page 801 (required)
- SIP: Configuring an Intercom Auto-Answer Line, page 803 (required)

SCCP: Configuring an Intercom Auto-Answer Line

To enable a two-way audio path between two phones, perform the following steps for each SCCP phone at both ends of the two-way voice path.

Restrictions

- 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.
- A separate configuration is required for each phone at both ends of the two-way voice path.

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.

	Command or Action	Purpose
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.
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 configuration mode and enters privileged EXEC mode.

SIP: Configuring an Intercom Auto-Answer Line

To enable the Intercom Auto-Answer feature for SIP phones, perform the following steps for each SIP phone at both ends of the two-way voice path.

Prerequisites

Cisco CME 3.4 or a later version.

Restrictions

- If a directory number is configured for intercom operation, it can be associated with only one Cisco Unified IP phone.
- A separate configuration is required for each phone at each end of the two-way voice path.

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 SIP phone, intercom line, voice port, or an MWI.

	Command or Action	Purpose
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.
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 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.A3D4.1234`	Explicitly identifies a locally available individual SIP 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 SIP 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 SIP phone being configured.
Step 11	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuration Examples for Intercom Lines

This section contains the following example:

- Intercom Lines: Example, page 805

Intercom Lines: Example

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
```

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 "Generating Configuration Files for Phones" on page 265.

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 "Configuring Paging" on page 831.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Intercom Lines

Table 50 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 50 lists the 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.

Table 50 Feature Information for Intercom Lines

Feature Name	Cisco Unified CME Version	Feature Information
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	The no-mute function was introduced.
	2.0	Intercom feature was introduced.

Configuring Loopback Call Routing

Last Updated: March 26, 2007

This chapter describes the loopback call-routing feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Loopback Call Routing" section on page 816.

Contents

Information About Loopback Call Routing

To enable loopback call routing, you should understand the following concept:

- Loopback Call Routing, page 809

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 "Configuring Call Transfer and Forwarding" on page 517.

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.

How to Configure Loopback Call Routing

This section contains the following tasks:

Enabling Loopback Call Routing

To enable loopback call-routing, perform the following steps for each ephone-dn that is part of the loopback-dn pair.

Restrictions

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.
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 by itself 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.

	Command or Action	Purpose
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. • **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 is used to specify 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.

	Command or Action	Purpose
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. • **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.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(config-ephone-dn)# end`	Exits to privileged exec mode.

Verifying Loopback Call Routing

Step 1 Use the **show running-config** or **show telephony-service ephone-dn** command to display ephone-dn configurations.

Configuration Examples for Loopback Call Routing

This section contains the following example:

- Enabling Loopback Call Routing: Example, page 814

Enabling Loopback Call Routing: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Loopback Call Routing

Table 51 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 51 lists the 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.

Table 51 Feature Information for Loopback Call Routing

Feature Name	Cisco Unified CME Version	Feature Information
Loopback Call Routing	2.0	Loopback call routing was introduced.

Configuring Music on Hold

Last Updated: May 24, 2007

This chapter describes the music on hold features in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Music on Hold" section on page 829.

Contents

Prerequisites for Music on Hold

- Phones receiving MOH in a system using G.729 require transcoding between G.711 and G.729. For information about transcoding, see "Configuring Transcoding Resources" on page 323.

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 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 an analog voice gateway (Cisco VG 224) 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.

Information About Music on Hold

To enable music on hold, you should understand the following concept:

- Music on Hold, page 818

Music on Hold

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.

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. For information about transcoding, see "Configuring Transcoding Resources" on page 323.

If the MOH audio stream is also identified as a multicast source, the Cisco Unified CME router additionally transmits the stream on the physical IP interfaces of the Cisco Unified CME router that you specify during configuration, which permits external devices to have access to it.

Certain IP phones do not support IP multicast and, therefore, do not support multicast MOH. You can disable multicast MOH to individual phones that do not support multicast. Callers hear a repeating tone when they are placed on hold.

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 an .au or .wav file held in router flash memory.
- 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.

If both are configured concurrently on the Cisco Unified CME router, the router seeks the live feed first. If the live feed is found, it displaces the audio file source. If the live feed is not found or fails at any time, the router falls back to the audio file source that was specified for MOH during configuration.

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 the "How to Configure Music on Hold" section on page 820.

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 Cisco 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 Cisco 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.

How to Configure Music on Hold

This section contains the following tasks:

- Configuring Music on Hold from an Audio File, page 820 (optional)
- Configuring Music on Hold from a Live Feed, page 822 (optional)
- Verifying Music on Hold, page 826 (optional)

Configuring Music on Hold from an Audio File

To configure MOH when you are using a file to supply the audio stream, perform the following steps.

Prerequisites

- 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.

Restrictions

- If MOH from an audio file and MOH from a live feed are both configured on the Cisco Unified CME router, 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.
- 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.

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. • *filename*—Source of the audio stream for MOH. **Note** If you specify a file with this command and later want to use a different file, you must disable use of the first file with the **no moh** command before configuring the second file.
Step 5	**multicast moh** *ip-address* **port** *port-number* [**route** *ip-address-list*] **Example:** `Router(config-telephony)# multicast moh 239.10.16.4 port 2123 route 10.10.29.17 10.10.29.33`	Specifies that the MOH audio stream should also be multicast as specified. **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*—Specifies that this audio stream is to be used for multicast and also for MOH, and specifies the 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. • **route**—(Optional) Specifies a 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.

	Command or Action	Purpose
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. 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. **Note** This command can also be used in an ephone template that is applied to one or more phones.
Step 9	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Configuring Music on Hold from a Live Feed

To configure music on hold from a live feed, perform the following steps.

Prerequisites

- 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.

Restrictions

- A foreign exchange station (FXS) port cannot be used for a live feed.
- The **signal loop-start live-feed** command for FXO ports is supported in Cisco IOS Release 12.4(11)XJ, 12.4(15)T, and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *port*
4. **input gain** *decibels*

5. **auto-cut-through** (E&M only)
6. **operation 4-wire** (E&M only)
7. **signal immediate** (E&M only)
8. **signal loop-start live-feed** (FXO only)
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. **Note** *Port* argument is platform-dependent; type **?** to display syntax. For more information, see the *Cisco IOS Voice Command Reference*.
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. Acceptable values are integers from –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.

	Command or Action	Purpose
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.
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.
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.

	Command or Action	Purpose
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`	Specifies that this ephone-dn is to be used for an incoming or outgoing call that is the source for an MOH stream. If this command is used without the **out-call** keyword, the MOH stream is received from an incoming call. • **out-call** *outcall-number*—(Optional) 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. • **ip** *ip-address*—(Optional) Indicates that this audio stream is to be used as a multicast source and also for MOH, and specifies the destination IP address for multicast. **Note** If you specify a multicast address with this command and a different multicast address with the **multicast moh** command under telephony-service configuration mode, you can send the MOH audio stream to two multicast addresses. • **port** *port-number*—(Optional) 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. • **route** *ip-address-list*—(Optional) Indicates specific router interfaces on which to transmit the IP multicast packets. Up to four IP addresses can be listed. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the **ip source-address** command.
Step 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.

	Command or Action	Purpose
Step 20	**multicast-moh** **Example:** `Router(config-ephone)# no multicast-moh`	(Optional) Enables multicast MOH on a phone. • This command is enabled by default. 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. **Note** This command can also be made part of an ephone template that is applied to one or more phones.
Step 21	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

Verifying Music on Hold

Step 1 Use the **show running-config** command to display the running configuration. MOH commands are listed in the telephony-service part 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 10.123.23.231 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 239.15.10.1 port 2000
 web admin system name admin1 password admin1
 dn-webedit
 time-webedit
 transfer-system full-consult
 secondary-dialtone 9
 fac custom callfwd all **1
 fac custom callfwd cancel **2
 fac custom pickup local **3
 fac custom pickup group *7
 fac custom pickup direct **5
 fac custom park *8
 fac custom dnd **7
 fac custom redial #8
 fac custom voicemail **9
 fac custom ephone-hunt join *3
 fac custom ephone-hunt cancel #3
 create cnf-files version-stamp Jan 01 2002 00:00:00
```

Step 2 Use the **show telephony-service** command to display only the telephony-service configuration information.

Configuration Examples for Music on Hold

This section contains the following examples:

- MOH from an Audio File: Example, page 827
- MOH from a Live Feed: Example, page 827

MOH from an Audio File: Example

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 additionally specifies a multicast address for the audio stream:

```
telephony-service
 moh minuet.wav
 multicast moh 239.23.4.10 port 2000
```

MOH from a Live Feed: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Music on Hold

Table 52 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 52 lists the 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.

Table 52 Feature Information for Music on Hold

Feature Name	Cisco Unified CME Version	Feature Information
Music on Hold	4.1	Music on hold for SIP phones was supported.
	4.0	• Music on hold was introduced for internal calls. • The ability to disable multicast MOH per phone was introduced.
	3.0	The ability to use a live audio feed as a multicast source was introduced.
	2.1	Music on hold from a live audio feed was introduced for external calls.
	2.0	Music on hold from an audio file was introduced for external calls.

Configuring Paging

Last Updated: March 26, 2007

This chapter describes the paging feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Paging" section on page 841.

Contents

Information About Paging

To enable paging, you should understand the following concept:

- Audio Paging, page 831

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 speakerphone 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.

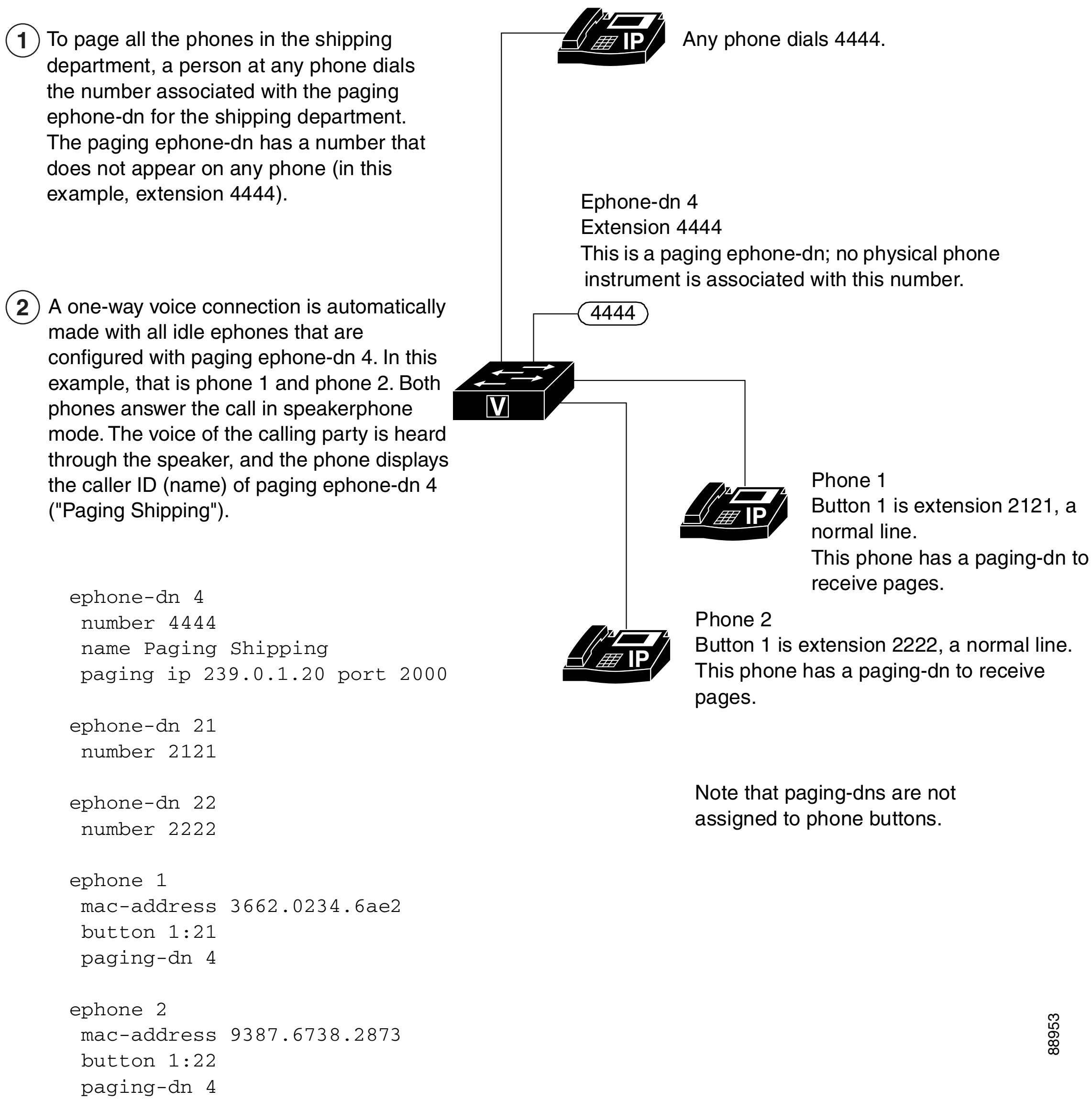
Audio paging provides a one-way voice path to the phones that have been designated to receive paging. It does not have a press-to-answer option like the intercom feature. A paging group is created using a dummy ephone-dn, known as the paging ephone-dn, that can be associated with any number of local 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 50 shows a paging group with two phones.

Figure 50 Paging Group



How to Configure Paging

This section contains the following tasks:

- Configuring a Simple Paging Group, page 833 (required)
- Configuring a Combined Paging Group, page 834 (optional)
- Verifying Paging, page 837 (optional)

Configuring a Simple Paging Group

To set up a paging number that relays incoming pages to a group of phones, perform the following steps.

Restrictions

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

Configuring a Combined Paging Group

To set up a combined paging group consisting of two or more simple paging groups, perform the following steps.

Prerequisites

Simple paging groups must be configured. See the "Configuring a Simple Paging Group" section on page 833.

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 the 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.
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.

	Command or Action	Purpose
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. List 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.
Step 10	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode.

	Command or Action	Purpose
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.

Verifying 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

This section contains the following examples:

- Simple Paging Group: Example, page 838
- Combined Paging Groups: Example, page 838

Simple Paging Group: Example

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
```

Combined Paging Groups: Example

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
```

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 "Configuring Intercom Lines" on page 799.

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 "Configuring Speed Dial" on page 893.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Paging

Table 53 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 53 lists the 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.

Table 53 Feature Information for Paging

Feature Name	Cisco Unified CME Version	Feature Information
Paging	2.0	Paging was introduced.

Configuring Presence Service

Last Updated: March 26, 2007

This module describes presence support in a Cisco Unified Communications Manager Express (Cisco Unified CME) system.

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Presence Service" section on page 864.

Contents

Prerequisites for Presence Service

- Cisco Unified CME 4.1 or a later version.
- Cisco IOS Release 12.4(11)XJ, 12.4(15)T, or a later release.
- Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE require firmware load 8.2(1) or a later version.

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

To configure presence service in a Cisco Unified CME system, you should understand the following concept:

- Presence Service, page 844

Presence Service

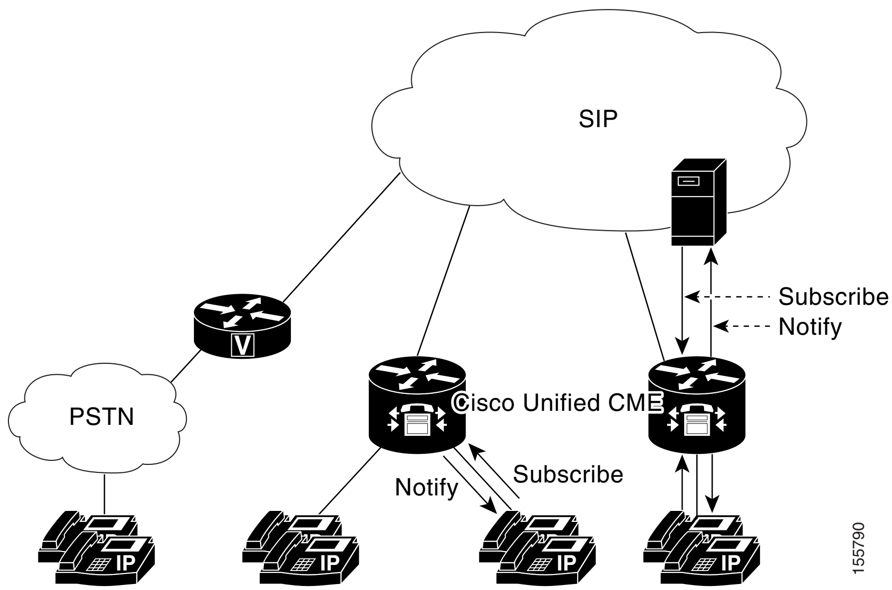
A presence service, as defined in RFC 2778 and RFC 2779, is a system for finding, retrieving, and distributing presence information from a source, called a presence entity (presentity), to an interested party called a watcher. When you configure presence in a Cisco Unified CME system with a SIP WAN connection, 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 51 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 51 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 the "How to Configure Presence Service" section on page 845.

How to Configure Presence Service

This section contains the following tasks:

Enabling Presence for Internal Lines

Perform the following steps to enable the router to accept incoming presence requests from internal watchers and SIP trunks.

Restrictions

- 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.

	Command or Action	Purpose
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.
Step 6	**presence** **Example:** `Router(config)# presence`	Enables presence service and enters presence configuration mode.
Step 7	**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 the "Enabling a SCCP Phone to Monitor BLF Status for Speed-Dials and Call Lists" section on page 849.
Step 8	**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 9	**end** **Example:** `Router(config-presence)# end`	Exits to privileged EXEC mode.

Enabling 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.

Restrictions

- 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*
   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.

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

Enabling a SCCP Phone to Monitor BLF Status for Speed-Dials and Call Lists

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.

Prerequisites

- Presence must be enabled on the Cisco Unified CME router. See the "Enabling Presence for Internal Lines" section on page 846.
- A directory number must be enabled as a presentity with the **allow watch** command to provide BLF status notification. See the "Enabling a Directory Number to be Watched" section on page 847.

Restrictions

BLF Call-List

- Supported only on Cisco Unified IP Phone 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.

BLF Speed-Dial

- Supported only on Cisco Unified IP Phone 7914, 7931, 7940, 7941G, 7941GE, 7960, 7961G, 7961GE, 7970G, and 7971GE.

Cisco Unified IP Phone 7931

- BLF status is displayed through monitor lamp only; BLF status icons are not displayed.

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*
6. **presence call-list**
7. **exit**
8. **telephony-service**
9. **create cnf-files**
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** *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* **Example:** `Router(config-ephone)# blf-speed-dial 3 3001 label sales`	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.
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 the "Enabling Presence for Internal Lines" section on page 846.
Step 7	**exit** **Example:** `Router(config-ephone)# exit`	Exits ephone configuration mode and enters privileged EXEC mode.
Step 8	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 9	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds the XML configuration files that are required for Cisco Unified CME phones.
Step 10	**restart** {**all** [*time-interval*] | *mac-address*} **Example:** `Router(config-telephony)# restart all`	Performs a fast reset of the specified phone or all phones associated with this Cisco Unified CME router. Does not contact the DHCP server. • **all**—Restarts all phones associated with a Cisco Unified CME router. • *time-interval*—(Optional) Time interval, in seconds, between the beginning of each phone restart. Range: 0 to 60. Default is 15. • *mac-address*—Restarts the phone that has the specified MAC address.
Step 11	**end** **Example:** `Router(config-telephony)# end`	Exits to privileged EXEC mode.

Enabling a SIP Phone to Monitor BLF Status for Speed-Dials and Call Lists

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.

Prerequisites

- Presence must be enabled on the Cisco Unified CME router. See the "Enabling Presence for Internal Lines" section on page 846.
- A directory number must be enabled as a presentity with the **allow watch** command to provide BLF status notification. See the "Enabling a Directory Number to be Watched" section on page 847.
- 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.

Restrictions

BLF Call-List

- Supported only on Cisco Unified IP Phone 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.

BLF Speed-Dial

- Supported only on Cisco Unified IP Phone 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.

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*
6. **presence call-list**
7. **exit**
8. **voice register global**
9. **mode cme**
10. **create profile**
11. **restart**
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 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* **Example:** `Router(config-register-pool)# blf-speed-dial 3 3001 label sales`	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.
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 the “Enabling Presence for Internal Lines” section on page 846.
Step 7	**exit** **Example:** `Router(config-register-pool)# exit`	Exits voice register pool configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 8	**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 9	**mode cme** **Example:** `Router(config-register-global)# mode cme`	Enables mode for provisioning SIP phones in Cisco Unified CME.
Step 10	**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 the **tftp-path** command.
Step 11	**restart** **Example:** `Router(config-register-global)# restart`	Performs a fast reset of all SIP phones associated with this Cisco Unified CME router. Phones contact the TFTP server for updated configuration information and reregister without contacting the DHCP server.
Step 12	**end** **Example:** `Router(config-register-global)# end`	Exits to privileged EXEC mode.

Configuring 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.

Prerequisites

Presence service must be enabled for internal lines. See the "Enabling Presence for Internal Lines" section on page 846.

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.
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.

	Command or Action	Purpose
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.

Verifying 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

Step 1 **debug presence** {**all** | **asnl** | **errors** | **event** | **info** | **timer** | **trace** | **xml**}

This command displays debugging information about the presence service.

```
Router# debug presence errors

*Sep  4 07:16:02.715: //PRESENCE:[0]:/presence_sip_line_update: SIP nothing to update
*Sep  4 07:16:02.723: //PRESENCE:[17]:/presence_handle_notify_done: sip stack response
code [29]
*Sep  4 07:16:02.723: //PRESENCE:[24]:/presence_handle_notify_done: sip stack response
code [29]
*Sep  4 07:16:02.791: //PRESENCE:[240]:/presence_handle_notify_done: sip stack response
code [17]
```

```
*Sep  4 07:16:02.791: //PRESENCE:[766]:/presence_handle_notify_done: sip stack response
code [17]
*Sep  4 07:16:04.935: //PRESENCE:[0]:/presence_sip_line_update: SIP nothing to update
*Sep  4 07:16:04.943: //PRESENCE:[17]:/presence_handle_notify_done: sip stack response
code [29]
*Sep  4 07:16:04.943: //PRESENCE:[24]:/presence_handle_notify_done: sip stack response
code [29]
*Sep  4 07:16:04.995: //PRESENCE:[240]:/presence_handle_notify_done: sip stack response
code [17]
*Sep  4 07:16:04.999: //PRESENCE:[766]:/presence_handle_notify_done: sip stack response
code [17]
```

Step 2 **debug ephone blf** [**mac-address** *mac-address*]

This command displays debugging information for BLF presence features.

```
Router# debug ephone blf

*Sep  4 07:18:26.307: skinny_asnl_callback: subID 16 type 4
*Sep  4 07:18:26.307: ASNL_RESP_NOTIFY_INDICATION
*Sep  4 07:18:26.307: ephone-1[1]:ASNL notify indication message, feature index 4, subID
[16]
*Sep  4 07:18:26.307: ephone-1[1]:line status 6, subID [16]
*Sep  4 07:18:26.307: ephone-1[1]:StationFeatureStatV2Message sent, status 2
*Sep  4 07:18:26.307: skinny_asnl_callback: subID 23 type 4
*Sep  4 07:18:26.307: ASNL_RESP_NOTIFY_INDICATION
*Sep  4 07:18:26.307: ephone-2[2]:ASNL notify indication message, feature index 2, subID
[23]
*Sep  4 07:18:26.311: ephone-2[2]:line status 6, subID [23]
*Sep  4 07:18:26.311: ephone-2[2]:StationFeatureStatV2Message sent, status 2
*Sep  4 07:18:28.951: skinny_asnl_callback: subID 16 type 4
*Sep  4 07:18:28.951: ASNL_RESP_NOTIFY_INDICATION
*Sep  4 07:18:28.951: ephone-1[1]:ASNL notify indication message, feature index 4, subID
[16]
*Sep  4 07:18:28.951: ephone-1[1]:line status 1, subID [16]
*Sep  4 07:18:28.951: ephone-1[1]:StationFeatureStatV2Message sent, status 1
*Sep  4 07:18:28.951: skinny_asnl_callback: subID 23 type 4
*Sep  4 07:18:28.951: ASNL_RESP_NOTIFY_INDICATION
*Sep  4 07:18:28.951: ephone-2[2]:ASNL notify indication message, feature index 2, subID
[23]
*Sep  4 07:18:28.951: ephone-2[2]:line status 1, subID [23]
*Sep  4 07:18:28.951: ephone-2[2]:StationFeatureStatV2Message sent, status 1
```

Configuration Examples for Presence

This section contains the following example:

- Presence in Cisco Unified CME: Example, page 859

Presence in Cisco Unified CME: Example

```
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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Presence Service

Table 54 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 54 lists the 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.

Table 54 Feature Information for Presence Service

Feature Name	Cisco Unified CME Version	Modification
Presence Service	4.1	Presence with BLF was introduced.

Configuring Ring Tones

Last Updated: March 26, 2007

This chapter describes ring tones features in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Ring Tones" section on page 874.

Contents

Information About Ring Tones

To enable distinctive ringing or customized ring tones, you should understand the following concepts:

- Distinctive Ringing, page 866
- Customized Ring Tones, page 866
- On-Hold Indicator, page 866

Distinctive Ringing

Distinctive ring is used to identify internal and external incoming calls. An internal calls 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 Ring Tones

Cisco Unified IP Phones have two default ring types: Chirp1 and Chirp2. Cisco Unified CME also supports customized ring tones using pulse code modulation (PCM) files.

An XML file called RingList.xml specifies the ring tone options available for the default ring on an IP phone registered to Cisco Unified CME. An XML file called DistinctiveRingList.xml specifies the ring tones 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 the "SCCP: Enabling On-Hold Indicator" section on page 870.

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.

How to Configure Ring Tones

This section contains the following tasks:

SCCP: Enabling Distinctive Ringing

To set the ring pattern for all incoming calls to a directory number, perform the following steps.

Prerequisites

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** **Example:** `Router> 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 29`	Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.

	Command or Action	Purpose
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.

SCCP: Enabling Customized Ring Tones

To create a customized ring tone, perform the following steps.

Prerequisites

Cisco Unified CME 4.0 or a later version.

SUMMARY STEPS

1. Create PCM file.
2. Edit RingList.xml and DistinctiveRingList.xml.
3. Copy PCM and XML files to system Flash.
4. **tftp-server**
5. Reboot phones.

DETAILED STEPS

Step 1 Create a PCM file for each customized ring tone (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
- µLaw 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 ring tone files. Select the customized ring by pressing the Settings button followed by the Ring Type menu option on a phone.

SCCP: Enabling 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**}
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`* [**`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`**} **Example:** `Router(config-ephone-dn)# hold-alert 15 idle`	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.

SIP: Enabling Distinctive Ringing

To set the ring pattern for distinguishing between external and internal incoming calls, perform the following steps.

Prerequisites

Cisco Unified CME 3.4 or a later version.

Restrictions

bellcore-dr1 to bellcore-dr5 are the only Telcordia options that are supported for SIP phones.

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`** **Example:** `Router> 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	**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 Ring Tones

This section contains the following examples:

- Distinctive Ringing for Internal Calls: Example, page 872
- On-Hold Indicator: Example, page 872

Distinctive Ringing for Internal Calls: Example

The following example sets distinctive ringing for internal calls on extension 2333.

```
ephone-dn 34
 number 2333
 ring internal
```

On-Hold Indicator: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Ring Tones

Table 55 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 55 lists the 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.

Table 55 Feature Information for Ring Tones

Feature Name	Cisco Unified CME Version	Feature Information
Distinctive Ringing	4.0	Supports ring tones 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 Ring Tones	4.0	Customized Ring Tones 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.

Customizing Soft Keys

Last Updated: June 20, 2007

This chapter describes the soft-key features in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Soft Keys" section on page 891.

Contents

Information About Soft Keys

To customize soft keys on IP phones, you should understand the following concepts:

Soft Keys on IP Phones

You can customize the display and order of soft keys that appear during various call states on individual IP phones. Soft keys that are appropriate in each call state are displayed by default. Using phone templates, you can delete soft keys that would normally appear or change the order in which the soft keys appear. For example, you might want to display the CFwdAll and Confrn soft keys on a manager's phone and remove these soft keys from a receptionist's phone.

You can modify soft keys 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 complete.
- Seized—When a caller is attempting a call but has not yet been connected.
- Ringing—For Cisco Unified CME 4.2 or a later version. After a call is received and before the call is connected.

Not all soft keys are available in all call states. Use the CLI help to see the available soft keys for each call state. The soft keys are as follows:

- Acct—Short for "account code." Provides access to configured accounts.
- Answer—Picks up incoming call.
- Callback—Requests callback notification when a busy called line becomes free.
- CFwdALL—Short for "call forward all." Forwards all calls.
- Confrn—Short for "conference." Connects callers to a conference call.
- 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, it places the phone into the ready status.
- Hold—Places an active call on hold and resumes the call.
- Login—Provides personal identification number (PIN) access to restricted phone features.
- 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.
- Trnsfer—Short for "call transfer." Transfers an active call to another extension.

You change the soft-key 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 ten 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 soft key display for IP phones running SIP is supported only for the Cisco Unified IP Phone 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.

For configuration information, see the "How to Customize Soft Keys" section on page 878.

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** soft key. 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** soft key, 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 Cisco Unified CME does not receive a #, each account code digit is processed only after a timer expires. The timer is 30 seconds for the first digit entered, then *x* seconds for each subsequent digit, where *x* 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 **show** output until after being processed.

Hookflash Soft Key

The Flash soft key provides hookflash functionality for calls made on FXO trunks. Certain public switched telephone network (PSTN) services, such as three-way calling and call waiting, require hookflash intervention from a phone user. A soft key, labeled Flash, provides this hookflash functionality for IP phones that use foreign exchange office (FXO) lines attached to the Cisco Unified CME system.

When a Flash soft key 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 soft key does not guarantee that hookflash-based services are accessible to the phone user.

For configuration information, see the "Enabling Flash Soft Key" section on page 884.

Feature Blocking

In Cisco Unified CME 4.0 and later versions, individual soft-key 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 soft key is not removed, but it does not function. For configuration information, see the "Configuring Feature Blocking" section on page 886.

To remove a soft-key display, use the appropriate **no softkeys** command. See the "SCCP: Modifying Soft-Key Display" section on page 878.

How to Customize Soft Keys

This section contains the following tasks:

SCCP: Modifying Soft-Key Display

To modify the display of soft-keys, perform the following steps.

Prerequisites

- Cisco CME 3.2 or a later version.
- Cisco Unified 4.2 or a later version to enable soft keys during the ringing call state.
- The HLog soft key must be enabled with the **hunt-group logout HLog** command before it will be displayed. For more information, see the "SCCP: Configuring Hunt Groups" section on page 614.
- The Flash soft key must be enabled with the **fxo hook-flash** command before it will be displayed. For configuration information, see the "Enabling Flash Soft Key" section on page 884.

Restrictions

- The third soft-key button on the Cisco Unified IP Phone 7905G and Cisco Unified IP Phone 7912G is reserved for the Message soft key. For these phones' templates, the third soft-key defaults to the Message soft key. For example, the **softkeys idle Redial Dnd Pickup Login Gpickup** command configuration displays, in order, the Redial, DND, Message, PickUp, Login, and GPickUp soft keys.
- The NewCall soft key cannot be disabled on the Cisco Unified IP Phone 7905G or Cisco Unified IP Phone 7912G.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-template** *template-tag*
4. **softkeys alerting** {[**Acct**] [**Callback**] [**Endcall**]}
5. **softkeys connected** {[**Acct**] [**Confrn**] [**Endcall**] [**Flash**] [**Hlog**] [**Hold**] [**Park**] [**Trnsfer**]}
6. **softkeys hold** {[**Newcall**] [**Resume**]}
7. **softkeys idle** {[**Cfwdall**] [**Dnd**] [**Gpickup**] [**Hlog**] [**Login**] [**Newcall**] [**Pickup**] [**Redial**]}
8. **softkeys seized** {[**Cfwdall**] [**Endcall**] [**Gpickup**] [**Hlog**] [**Pickup**] [**Redial**]}
9. **softkeys ringing** {[**Answer**] [**Dnd**] [**HLog**]}
10. **exit**
11. **ephone** *phone-tag*
12. **ephone-template** *template-tag*
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	**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 soft-key display during the alerting 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	**softkeys connected** {[**Acct**] [**Confrn**] [**Endcall**] [**Flash**] [**Hlog**] [**Hold**] [**Park**] [**Trnsfer**]} **Example:** `Router(config-ephone-template)# softkeys connected Endcall Hold Transfer Hlog`	(Optional) Configures an ephone template for soft-key display during the call-connected 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.

	Command or Action	Purpose
Step 6	**softkeys hold** {[**Newcall**] {**Resume**]} **Example:** `Router(config-ephone-template)# softkeys hold Resume`	(Optional) Configures an ephone template for soft-key display during the call-hold 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 7	**softkeys idle** {[**Cfwdall**] [**Dnd**] [**Gpickup**] [**Hlog**] [**Login**] [**Newcall**] [**Pickup**] [**Redial**]} **Example:** `Router(config-ephone-template)# softkeys idle Newcall Redial Pickup Cfwdall Hlog`	(Optional) Configures an ephone template for soft-key display during the idle 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 8	**softkeys seized** {[**Cfwdall**] [**Endcall**] [**Gpickup**] [**Hlog**] [**Pickup**] [**Redial**]} **Example:** `Router(config-ephone-template)# softkeys seized Endcall Redial Pickup Cfwdall Hlog`	(Optional) Configures an ephone template for soft-key display during the seized 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 9	**softkeys ringing** {[**Answer**] [**Dnd**] [**HLog**]} **Example:** `Router(config-ephone-template)# softkeys ringing Answer Dnd Hlog`	(Optional) Configures an ephone template for soft-key display during the ringing 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 10	**exit** **Example:** `Router(config-ephone-template)# exit`	Exits ephone-template configuration mode.
Step 11	**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 12	**ephone-template** *template-tag* **Example:** `Router(config-ephone)# ephone-template 15`	Applies an ephone template to the ephone that is being configured.
Step 13	**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 the "SCCP: Generating Configuration Files for SCCP Phones" section on page 267.

SIP: Modifying Soft-Key Display

To modify the display of soft keys on SIP phones for different call states, perform the following steps.

Prerequisites

Cisco Unified CME 4.1 or a later version.

Restrictions

- This feature is supported only for Cisco Unified IP Phones 7911G, 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE.
- You can download a custom soft key XML file from a TFTP server, however if the soft key XML file contains an error, the soft keys might not work properly on the phone. We recommend the following procedure for creating a soft key template in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register template** *template-tag*
4. **softkeys connected** {[**Confrn**] [**Endcall**] [**Hold**] [**Trnsfer**]}
5. **softkeys hold** {[**Newcall**] [**Resume**]}
6. **softkeys idle** {[**Cfwdall**] [**Newcall**] [**Redial**]}
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.
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**]} **Example:** `Router(config-register-template)# softkeys connected Endcall Hold Transfer`	(Optional) Configures an SIP phone template for soft-key display during the call-connected state. • You can enter 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	**softkeys hold** {[**Newcall**] {**Resume**]} **Example:** `Router(config-register-template)# softkeys hold Resume`	(Optional) Configures a phone template for soft-key display during the call-hold state. • Default is that the NewCall and Resume soft keys are displayed in alphabetical order. • Any soft key that is not explicitly defined is disabled.
Step 6	**softkeys idle** {[**Cfwdall**] [**Newcall**] [**Redial**]} **Example:** `Router(config-register-template)# softkeys idle Newcall Redial Cfwdall`	(Optional) Configures a phone template for soft-key display during the idle state. • You can enter 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 7	**softkeys seized** {[**Cfwdall**] [**Endcall**] [**Redial**]} **Example:** `Router(config-register-template)# softkeys seized Endcall Redial Cfwdall`	(Optional) Configures a phone template for soft-key display during the seized state. • You can enter 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 8	**exit** **Example:** `Router(config-register-template)# exit`	Exits voice register template configuration mode.

	Command or Action	Purpose
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* **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 11	**end** **Example:** `Router(config-register-pool)# end`	Exits 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 the "SIP: Generating Configuration Profiles for SIP Phones" section on page 270.

Verifying Soft-Key Configuration

Step 1 **show running-config**

Use this command to verify your configuration. In the following example, the soft-key display is modified in phone template 7 and the template is applied to SIP phone 2. All other phones use the default arrangement of soft keys.

```
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
!
!
voice register template  7
 session-transport tcp
 softkeys hold  Resume Newcall
 softkeys idle  Newcall Redial Cfwdall
 softkeys connected  Endcall Trnsfer Confrn Hold
 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*

This command displays 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
  softkey hold  Resume Newcall
  softkey idle  Newcall Redial Cfwdall
```

Enabling Flash Soft Key

To enable the flash soft key, perform the following steps.

Restrictions

The IP phone must support soft-key display.

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 soft key on phones that support soft-key display, on PSTN calls using an FXO port. **Note** The Flash soft key 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.

Verifying Flash Soft-Key Configuration

Step 1 Use the **show running-config** command to display an entire configuration, including Flash soft key, which is listed in the telephony-service portion of the output.

```
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.

Configuring Feature Blocking

To configure feature blocking for SCCP phones, perform the following steps.

Prerequisites

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.

	Command or Action	Purpose
Step 4	**features blocked** [**CFwdAll**] [**Confrn**] [**GpickUp**] [**Park**] [**PickUp**] [**Trnsfer**] **Example:** `Router(config-ephone-template)# features blocked Park Trnsfer`	Prevents the specified soft key from invoking its feature. • **CFwdAll**—Call forward all calls. • **Confrn**—Conference. • **GpickUp**—Group call pickup. • **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.

Verifying Feature Blocking

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.

Configuration Examples for Soft-Keys

This section contains the following examples:

- Modifying Soft-Key Display: Example, page 888
- Modifying the HLog Soft Key for Ephone Hunt Groups: Example, page 889
- Enabling Flash Soft Key for PSTN Calls: Example, page 889
- Park and Transfer Blocking: Example, page 889
- Conference Blocking: Example, page 889

Modifying Soft-Key Display: Example

The following example modifies soft-key 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 soft-key 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 10
 ephone-template 2

ephone 13
 ephone-template 1

ephone 15
 ephone-template 1

ephone 34
 ephone-template 2
```

Modifying the HLog Soft Key for Ephone Hunt Groups: Example

The following example establishes the appearance and order of soft keys 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 soft keys 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
```

Enabling Flash Soft Key for PSTN Calls: Example

The following example enables the Flash soft key for PSTN calls through an FXO voice port.

```
telephony-service
 fxo hook-flash
```

Park and Transfer Blocking: Example

The following example blocks the use of Park and Transfer soft keys on extension 2333.

```
ephone-template 1
 features blocked Park Trnsfer

ephone-dn 2
 number 2333

ephone 3
 button 1:2
 ephone-template 1
```

Conference Blocking: Example

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
```

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. For more information, see "Generating Configuration Files for Phones" on page 265.

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 "Creating Templates" on page 927.

HLog Soft Key

The HLog soft key must be enabled with the **hunt-group logout HLog** command before it will be displayed. For more information, see "Configuring Call-Coverage Features" on page 581.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Soft Keys

Table 56 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 56 lists the 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.

Table 56 Feature Information for Soft Keys

Feature Name	Cisco Unified CME Version	Feature Information
Account Code Entry	3.0	Account code entry was introduced.
Feature Blocking	4.0	Feature blocking was introduced.
Flash Soft Key	3.0	Flash soft key was introduced.
Soft-Key Display	4.1	Configurable soft key 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 soft key was added to the connected, idle, and seized call states. • The ability to customize soft-key display in the hold call state was added.
	3.2	Configurable soft-key display (the ability to customize soft-key display in the alerting, connected, idle, and seized call states) was introduced.

Configuring Speed Dial

Last Updated: May 14, 2007

This chapter describes the speed dial support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Speed Dial" section on page 912.

Contents

Information About Speed Dial

To enable speed dial, you should understand the following concepts:

- Speed Dial Summary, page 894
- Speed Dial Buttons and Abbreviated Dialing, page 895
- Bulk-Loading Speed Dial Numbers, page 895
- Monitor-Line Button for Speed Dial, page 896
- DSS (Direct Station Select) Service, page 897

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 57.

Table 57 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.	Enabling a Local Speed Dial Menu, page 898.
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.	• SCCP: Enabling a Personal Speed Dial Menu, page 901 • SIP: Configuring a Personal Speed-Dial Menu, page 907.
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. Analog phone users invoke speed dial by entering an asterisk and the speed-dial code (tag) number of the desired entry.	• SCCP: Defining Speed-Dial Buttons and Abbreviated Dialing, page 902 • SIP: Defining Speed-Dial Buttons, page 906.
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*]	SCCP: Enabling Bulk-Loading Speed-Dial, page 904.

Table 57 Speed Dial Types

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.	SCCP: Enabling DSS Service, page 900.

Speed Dial Buttons and Abbreviated Dialing

In a Cisco Unified CME system, each phone can have up to 33 local speed-dial numbers (codes 1 to 33), 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 33 for local, per-phone speed-dial numbers and use codes 34 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 the "SCCP: Defining Speed-Dial Buttons and Abbreviated Dialing" section on page 902.

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 58 explains the fields in a bulk speed-dial list entry.

Table 58 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 the "SCCP: Enabling Bulk-Loading Speed-Dial" section on page 904.

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 the "Enabling a Local Speed Dial Menu" section on page 898.

How to Configure Speed Dial

This section contains the following tasks:

Enabling 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:

Prerequisites

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 the *Cisco IP Phone Services Application Development Notes*.

Restrictions

- 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 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.

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.
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.

SCCP: Enabling 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.

Prerequisites

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.

SCCP: Enabling a Personal Speed Dial Menu

To enable a personal speed-dial menu, perform the following steps.

Restrictions

- A personal speed-dial menu is available only on Cisco Unified IP Phones 7940, 7960, 7960G, 7970G and 7971G-GE.

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 sequence number for the phone for which you want to program personal speed-dial numbers.

	Command or Action	Purpose
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 IP phone. • *dial-tag*—Unique identifier to identify this entry during configuration. Range is 1 to 24. • *number*—Telephone number or extension to be dialed. • **name** *name-string*—Label to appear in the Personal Speed Dial menu, containing a string of a maximum of 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.

SCCP: Defining Speed-Dial Buttons and Abbreviated Dialing

To define speed-dial buttons and abbreviated dialing codes, perform the following steps for each speed-dial definition to be configured.

Restrictions

- On-hook abbreviated dialing using the Abbr soft key is supported only on the following phone types:
  - 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. **exit**

6. **telephony-service**
7. **directory entry** {*directory-tag number* **name** *name* | **clear**}
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 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.

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

SCCP: Enabling Bulk-Loading Speed-Dial

To enable bulk-loading speed-dial numbers, perform the following steps:

Prerequisites

- 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.

Restrictions

- Bulk speed dial is not supported on FXO trunk lines.

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. **exit**
7. **ephone** *phone-tag*
8. **bulk-speed-dial list** *list-id 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.

	Command or Action	Purpose
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. • *location*—Location of the bulk speed-dial text file in URL format. Valid storage locations are TFTP, Slot 0/1, and flash memory.
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	**exit** **Example:** `Router(config-telephony)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 7	**ephone** *phone-tag* **Example:** `Router(config)# ephone 25`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 8	**bulk-speed-dial list** *list-id location* **Example:** `Router(config-ephone)# bulk-speed-dial list 7 flash:lmi_sd_list_08_24_95.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. • *location*—Location of the bulk speed-dial text file in URL format. Valid storage locations are TFTP, Slot 0/1, and flash memory.
Step 9	**end** **Example:** `Router(config-ephone)# end`	Returns to privileged EXEC mode.

SCCP: Verifying Bulk Speed-Dial Parameters

show telephony-service bulk-speed-dial

Use this command to display information on speed-dial lists.

```
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)
```

SIP: Defining Speed-Dial Buttons

To define speed-dial buttons for Cisco SIP IP phones, perform the following steps.

Prerequisites

Cisco CME 3.4 or a later version.

Restrictions

- Certain SIP IP 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.

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** **Example:** `Router> 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 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"
```

SIP: Configuring a Personal Speed-Dial Menu

To define up to 24 personal speed-dial numbers for a SIP phone, perform the following steps.

Prerequisites

- Cisco Unified CME 4.1 or a later version.

Restrictions

- Cisco Unified IP Phone 7941G, 7941GE, 7961G, 7961GE, 7970G, and 7971GE—Personal speed-dial numbers can only be created in Cisco Unified CME, using this procedure.

- Cisco Unified IP Phone 7905, 7912, 7940, and 7960—Speed dial numbers can only be created by the user directly on the phone and not in Cisco Unified CME.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool** *pool-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	`voice register pool` *pool-tag* **Example:** `Router(config-register-pool)# 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	`fastdial` *dial-tag number* [`name` *name-string*] **Example:** `Router(config-register-pool)# fastdial 1 5552 name Sales`	Creates a personal speed-dial number on this SIP phone. • *dial-tag*—Unique number to identify this entry during configuration. Range: 1 to 24. • *number*—Telephone number or extension to be dialed. • **name** *name-string*—(Optional) Label to appear in the Personal Speed Dial menu, containing a string of a maximum of 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. • Repeat this command for each personal speed-dial number that you want to create on this phone.
Step 5	`end` **Example:** `Router(config-register-pool)# end`	Exits to privileged EXEC mode.

Configuration Examples for Speed Dial

This section contains the following examples:

- Enabling a Local Speed Dial Menu: Example, page 909
- Personal Speed Dial Menu: Example, page 909
- Speed-Dial Buttons and Abbreviated Dialing: Example, page 910
- Bulk-Loading Speed Dial: Example, page 910

Enabling a Local Speed Dial Menu: Example

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>
```

Personal Speed Dial Menu: Example

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
```

Speed-Dial Buttons and Abbreviated Dialing: Example

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
```

Bulk-Loading Speed Dial: Example

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
```

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 "Resetting and Restarting Phones" on page 277.

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 "Configuring Call Transfer and Forwarding" on page 517.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Speed Dial

Table 59 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CallManager Express and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 59 lists the 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.

Table 59 Feature Information for Speed Dial

Feature Name	Cisco Unified CME Version	Feature Information
Speed 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.

Configuring Video Support for SCCP-Based Endpoints

Last Updated: September 10, 2007

This chapter describes the video support for SCCP-based endpoints in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the Feature Information for Video Support for SCCP-Based Endpoints, page 925.

Contents

Prerequisites for Video Support for SCCP-Based Endpoints

- H.323 or SIP network for voice calls is operational.
- Cisco IOS Release 12.4(9)T or a later version.
- Cisco Unified CME version is 4.0 or later version.
- Cisco Unified Communications Manager version is 4.0 or later.
- Cisco Unified IP phones are registered in Cisco Unified CME. Use the **show ephone registered** command to verify ephone registration.
- Connection between the Cisco Unified Video Advantage 1.02 or a later version and the Cisco Unified IP phone is up.

From a PC with Cisco Unified Video Advantage version 1.02 or later installed, ensure that the line between the Cisco Unified Video Advantage and the Cisco Unified IP phone is green. For more information, see the *Cisco Unified Video Advantage User Guide.*

- Correct video firmware is installed on the Cisco Unified IP phone. Use the **show ephone phone-load** command to view current ephone firmware. The following lists the minimum firmware version for video-enabled Cisco Unified IP phones:
  - Cisco Unified IP Phone 7940G 6.0(4)
  - Cisco Unified IP Phone 7960G 6.0(4)
  - Cisco Unified IP Phone 7970G 7.0(3)
  - Cisco Unified IP Phone 7941G 7.0(3)
  - Cisco Unified IP Phone 7961G 7.0(3)

Note Other video-enabled endpoints, if registered with Cisco Unified Communications Manager, can place a video call to one of the Cisco Unified IP phones listed above if it is registered with Cisco Unified CME.

Restrictions for Video Support for SCCP-Based Endpoints

- This feature supports only the following video codecs:
  - H.261
  - H.263
- 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.
- Video capabilities are configured per ephone, not per line.
- All call feature controls (for example, mute and hold) apply to both audio and video calls, if applicable.
- This feature does not support the following:
  - Dynamic addition of video capability—The video capability must be present *before* the call setup starts to allow the video connection.
  - T-120 data connection between two SCCP endpoints
  - Video security
  - Far-end camera control (FECC) for SCCP endpoints
  - Video codec renegotiation—The negotiated video codec must match or the call falls back to audio-only. The negotiated codec for the existing call can be used for a new call.

- Video codec transcoding
- SIP endpoints— When a video-capable SCCP endpoint connects to a SIP endpoint, the call falls back to audio-only.
- Video conferencing—The call falls back to audio-only.
- Features, such as conferencing, that mix the audio streams in Cisco Unified CME—In those cases, the call falls back to audio-only.
- Video supplementary services between Cisco Unified CME and Cisco Unified Communications Manager.

- If the Cisco Unified Communications Manager is configured for Media Termination Point (MTP) transcoding, a video call between Cisco Unified CME and Cisco Unified Communications Manager is not supported.
- Video telephony is not supported with 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 H323 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.

Information About Video Support for SCCP-Based Endpoints

To configure video support for SCCP endpoints, you should understand the following concepts:

- Video Support Overview, page 916
- Matching Endpoint Capabilities, page 916
- Retrieving Video Codec Information, page 916
- Call Fallback to Audio-Only, page 916
- Call Setup for Video Endpoints, page 917
- Flow of the RTP Video Stream, page 917

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 not enabled 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 ephones associated with a Cisco Unified CME router and then enable video on each ephone individually.

Video parameters, like maximum bit rate, are set in video configuration mode.

Note After video is enabled globally, all video-capable ephones display the video icon.

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 (that exist on the same router), video call setup uses all existing audio-call-setup handling, except during media setup. During media setup, a message is sent to establish the video-media-path. If the endpoint responds, the video-media-path is established and a start-multimedia-transmission function is called.

Call Setup Between SCCP and H.323 Endpoints

Call setup between SCCP and H.323 endpoints is the same as it is between SCCP endpoints except that if video capability is selected, the event is posted to the H.323 call leg to send out a video open logical channel (OLC) and the gateway generates an OLC for the video channel. Because the router needs to both terminate and originate the media stream, video must be enabled on the router before call setup begins.

Call Setup Between Two SCCP Endpoints Across an H.323 Network

If call setup between SCCP endpoints occurs across an H.323 network, the setup is a combination of the processes listed in the previous two sections. The router controls the video media setup between the two endpoints, and the event is posted to the H.323 call leg so that the gateway can generate an OLC.

Flow of the RTP Video Stream

For video streams between two local SCCP endpoints, the Real-Time Transport Protocol (RTP) stream is in flow-around mode. For video streams between SCCP and H.323 endpoints or two SCCP endpoints on different Cisco Unified CME routers, the RTP stream is in flow-through mode.

- Media flow-around mode enables RTP packets to stream directly between the endpoints of a VoIP call without the involvement of the gateway. By default, the gateway receives the incoming media, terminates the call, and then reoriginates it on the outbound call leg. In flow-around mode, only signaling data is passed to the gateway, improving scalability and performance.

- 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 show in the following sample output.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   102     103        18714    18158  10.1.1.1        192.168.1.1
2   105     104        17252    19088  10.1.1.1        192.168.1.1
Found 2 active RTP connections
============================
```

How to Configure Video for SCCP-Based Endpoints

This section contains the following tasks:

- Enabling Slow Connect Procedures for H.323 Endpoints, page 918 (required)
- Setting Video Parameters, page 919 (optional)
- Enabling Video Capabilities on a Specific Phone, page 920 (required)

Enabling Slow Connect Procedures for H.323 Endpoints

Video streams require slow-connect procedures for Cisco Unified CME. H.323 endpoints also require slow-connect because the endpoint capability match occurs after the connect message. To enable slow connect procedures in Cisco Unified CME for H.323 endpoints, perform the following steps.

Note For more information on slow-connect procedures, see *Configuring Quality of Service for Voice*.

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.
Step 6	**end** **Example:** `Router(config-serv-h323)# end`	Returns to privileged EXEC mode.

Setting Video Parameters

To 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.
Step 4	**service phone videoCapability {0 | 1}** **Example:** `Router(config-telephony)# service phone videoCapability 1`	(Optional) Disables or enables video capability parameter for all applicable IP phones associated with Cisco Unified CME router. • The parameter name is word and case-sensitive. • **0**—Disable. • **1**—Enable (Default). **Note** This command can also be configured in ephone-template configuration mode and applied to one or more phones.
Step 5	**video** **Example:** `Router(config-telephony)# video`	Enters video configuration mode.
Step 6	**maximum bit-rate** *value* **Example:** `Router(conf-tele-video)# maximum bit-rate 256`	Sets the maximum IP phone video bandwidth, in kbps. • *value*—Range 0 to 10000000. Default: 10000000.
Step 7	**end** **Example:** `Router(conf-tele-video)# end`	Returns to privileged EXEC mode.

Enabling Video Capabilities on a Specific Phone

To enable video for each video-capable SCCP phone associated with a Cisco Unified CME router, perform the following steps.

Prerequisites

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. The maximum number is platform-dependent.

	Command or Action	Purpose
Step 4	**video** **Example:** `Router(config-ephone)# video`	Enables video capabilities on the specified ephone.
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 "Generating Configuration Files for Phones" on page 265.

Verifying Video Support for SCCP-Based Endpoints

Step 1 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:

```
telephony-service
 video
  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-Based Endpoints

Step 1 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).

Step 2 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.

Step 3 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**—Displays the status of registered ephones.
- **show voip rtp connections**—Displays information about RTP named-event packets, such as caller ID number, IP address, and port for both the local and remote endpoints.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*

Related Topic	Document Title
Cisco IOS configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Software Releases 12.4T Configuration Guides*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Video Support for SCCP-Based Endpoints

Table 60 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The following table lists the 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.

Table 60 Feature Information for Video Support for SCCP-Based Endpoints

Feature Name	Cisco Unified CME Version	Feature Information
Video Support for SCCP-Based Endpoints	4.0	Video support for SCCP-based endpoints was introduced.

Creating Templates

Last Updated: March 26, 2007

This chapter describes templates support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Creating Templates" section on page 937.

Contents

Information About Templates

To enable templates you should understand the following concepts:

- Phone Templates, page 928
- Ephone-dn Templates, page 928

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 soft-key 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.

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 IP 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.

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.

Note The features that can be implemented using ephone-dn templates are available in the CLI help by entering a question mark:

```
Router(config)# ephone-dn-template 1
Router(config-ephone-dn-template)# ?
```

How to Configure Templates

This section contains the following tasks:

- SCCP: Enabling Ephone Templates, page 929
- SCCP: Enabling Ephone-dn Templates, page 930
- SCCP: Verifying Templates, page 931
- SIP: Creating and Applying Templates to SIP Phones, page 932

SCCP: Enabling Ephone Templates

To create an ephone template and apply it to a phone, perform the following steps:

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. See the CLI help 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.

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

SCCP: Enabling Ephone-dn Templates

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. See the CLI help 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.

SCCP: Verifying Templates

To view the configuration of a template, and verify to which phone or directory number a template is applied, perform the following steps.

SUMMARY STEPS

1. **show telephony-service ephone**
2. **show telephony-service ephone-template**
3. **show telephony-service ephone-dn**
4. **show telephony-service ephone-dn-template**

DETAILED 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.

SIP: Creating and Applying Templates to SIP Phones

To create templates of common features and softkeys that can be applied to individual Cisco SIP IP phones, follow the steps in this section.

Prerequisites

- 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`	Exits configuration mode and enters 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

This section contains the following examples:

- Using Ephone Template to Block The Use of Park and Transfer Soft Keys, page 934
- Using Ephone-dn Template to Set Call Forwarding, page 935

Using Ephone Template to Block The Use of Park and Transfer Soft Keys

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
```

Using Ephone-dn Template to Set Call Forwarding

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

Soft-Key Display

The display of soft keys during different call states is managed using ephone templates. For more information, see "Customizing Soft Keys" on page 875.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Creating Templates

Table 61 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 61 lists the 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.

Table 61 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 IP phones directly connected to a Cisco Unified CME router.

Modifying Cisco Unified IP Phone Options

Last Updated: May 22, 2007

This chapter describes the screen and button features available for Cisco Unified IP phones connected to Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Cisco Unified IP Phone Options" section on page 963.

Contents

Information About Cisco Unified IP Phone Options

To enable IP phone options, you should understand the following concepts:

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

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.

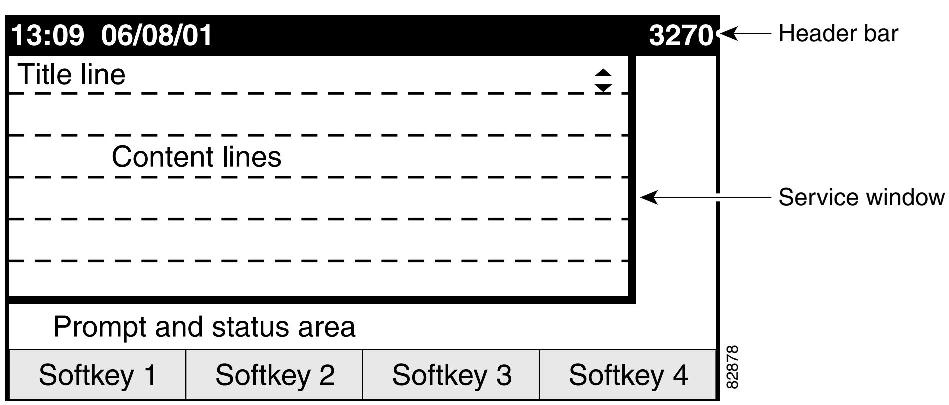
For configuration, see the "SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G" section on page 943.

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 52. 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 52 Cisco Unified IP Phone Display



Phone Labels

Pone 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 the "SCCP: Creating Labels for Directory Numbers" section on page 947 or the "SIP: Creating Labels for Directory Numbers" section on page 949.

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 the "SCCP: Modifying Vendor Parameters for All Phones" section on page 956. For configuration information for individual phones, see the "SCCP: Modifying Vendor Parameters For a Specific Phone" section on page 957.

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 customized feature buttons allows you to specify alternative XML files to access using the feature buttons on IP phones.

The Cisco Unified IP Phones 7940, 7940G, 7960, and 7960G have customized feature buttons that invoke noncall-related programmable services. The four buttons—Services, Directories, Messages, and Information (the i button)—are linked to appropriate feature operations through programmable URLs. The fifth button—Settings—is managed entirely by the phone. Operation of these services is determined by the IP phone capabilities and the content of the referenced URL.

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.

How to Configure Cisco Unified IP Phone Options

This section contains the following tasks:

Button Layout for Cisco Unified IP Phone 7931G

- SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G, page 943 (required)

Header Bar Display

- SCCP: Modifying Header Bar Display, page 944 (required)
- SIP: Modifying Header Bar Display, page 945 (required)
- Verifying Header Bar Display, page 947 (optional)
- Troubleshooting Header Bar Display, page 947 (optional)

Labels for Directory Numbers

- SCCP: Creating Labels for Directory Numbers, page 947 (required)
- SIP: Creating Labels for Directory Numbers, page 949 (required)
- Verifying Labels, page 950 (optional)

System Message Display

- SCCP: Modifying System Message Display, page 950 (required)
- Verifying System Message Display, page 952 (optional)
- Troubleshooting System Message Display, page 952 (optional)

URLs for Feature Buttons

- SCCP: Provisioning URLs for Feature Buttons, page 953 (required)
- SIP: Provisioning URLs for Feature Buttons, page 954 (required)
- Troubleshooting URL Provisioning for Feature Buttons, page 955 (optional)

Programmable VendorConfig Parameters

- SCCP: Modifying Vendor Parameters for All Phones, page 956 (optional)
- SCCP: Modifying Vendor Parameters For a Specific Phone, page 957 (optional)
- Troubleshooting Vendor Parameter Configuration, page 959 (optional)

SCCP: Selecting Button Layout for a Cisco Unified IP Phone 7931G

To select a fixed-button layout for a Cisco Unified IP Phone 7931G, perform the following steps.

Prerequisites

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 set** *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.

	Command or Action	Purpose
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.
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 "Generating Configuration Files for Phones" on page 265.

SCCP: Modifying Header Bar Display

To modify the phone header bar display, perform the following steps.

Prerequisites

Directory number to be modified is already configured. For configuration information, see "SCCP: Creating Directory Numbers" on page 177.

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 "Generating Configuration Files for Phones" on page 265.

SIP: Modifying Header Bar Display

To modify the phone header bar display on supported SIP phones, perform the following steps.

Prerequisites

- Cisco CME 3.4 or a a later version.

Restrictions

- This feature is supported only on Cisco Unified IP Phone 7940, 7940G, 7960, and 7960G.

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.
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 the "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

Verifying Header Bar Display

Step 1 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
 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

Step 1 **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
```

SCCP: Creating Labels for Directory Numbers

To create a label to display in place of the number next to a line button, perform the following steps.

Prerequisites

Directory number for which the label is to be created is already configured. For configuration information, see "SCCP: Creating Directory Numbers" on page 177.

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.
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 the "Generating Configuration Files for Phones" on page 265.

SIP: Creating Labels for Directory Numbers

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.

Prerequisites

- 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 "SIP: Creating Directory Numbers" on page 181.

Restrictions

- Only one label is permitted per directory number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** *dn-tag*
4. **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	`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.

	Command or Action	Purpose
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 the "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

Verifying Labels

Step 1 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
```

SCCP: Modifying System Message Display

To modify the system message display on phone screen, perform the following steps.

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)#`	Enters telephony-service configuration mode.
Step 4	**system message** *text-message* **Example:** `Router(config-telephony)# system message ABC Company`	Defines a text message to display when a phone is idle. • *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 "SCCP: Using the reset Command" on page 279.

Verifying System Message Display

Step 1 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

Step 1 Ensure that the HTTP server is enabled.

SCCP: Provisioning URLs for Feature Buttons

To customize URLs for feature buttons in the Sep*.conf.xml configuration file for SCCP IP phones, perform the following steps.

Restrictions

- 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)#`	Enters telephony-service configuration mode.

	Command or Action	Purpose
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 feature buttons on an IP phone: Directories, Information, Messages, and Services. • 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 or for the phones to register with Cisco Unified Communications Manager.
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 the "Generating Configuration Files for Phones" on page 265.

SIP: Provisioning URLs for Feature Buttons

To customize URLs for feature buttons SEPDEFAULT.cnf configuration profile for SIP IP phones, perform the following steps.

Prerequisites

- Cisco CME 3.4 or a later version.

Restrictions

- Operation of these services is determined by the Cisco Unified IP phone capabilities and the content of the specified URL.
- Provisioning a URL is supported only for Services and Directories feature buttons on SIP phones.
- Programmable Directories and Services feature buttons are supported only on the Cisco Unified IP Phone 7960, 7960G, 7940, and 7940G.
- 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. **voice register global**

4. **url** {**directory** | **service**} *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	**voice register global** **Example:** `Router(config)#`	Enters telephony-service configuration mode.
Step 4	**url** {**directory** | **service**} *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`	Associates a URL with the programmable feature buttons on SIP phones.
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 the "SIP: Generating Configuration Profiles for SIP Phones" on page 270.

Troubleshooting URL Provisioning for Feature Buttons

Step 1 Ensure the HTTP server is enabled and that there is communication between the Cisco Unified CME router and the server.

SCCP: Modifying Vendor Parameters for All 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.

Restrictions

- 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.

	Command or Action	Purpose
Step 4	**service phone** *parameter-name parameter-value* **Example:** `Router(config-telephony)# service phone daysBacklightNotActive 1,2,3,4,5,6,7` `Router(config-telephony)# service phone backlightOnTime 07:30` `Router(config-telephony)# service phone backlightOnDuration 10:00` `Router(config-telephony)# service phone backlightIdleTimeout 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 the *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.
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 the "Generating Configuration Files for Phones" on page 265.

SCCP: Modifying Vendor Parameters For a Specific Phone

To configure parameters in the vendorConfig section of the Sep*.conf.xml configuration file for an individual SCCP phone, perform the following steps.

Restrictions

- Cisco Unified CME 4.0 or a later version.
- System must be configured to for per-phone configuration files. For configuration information, see "SCCP: Defining Per-Phone Configuration Files and Alternate Location" on page 147.
- 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-ephone-template)# service phone daysBacklightNotActive 1,2,3,4,5,6,7` `Router(config-ephone-template)# service phone backlightOnTime 07:30` `Router(config-ephone-template)# service phone backlightOnDuration 10:00` `Router(config-ephone-template)# service phone backlightIdleTimeout 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 the "Generating Configuration Files for Phones" on page 265.

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

```
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.

Configuration Examples for Cisco Unified IP Phone Options

This section contains the following examples:

Text Labels for Ephone-dns: Example

The following example creates text labels for two ephone-dns:

```
ephone-dn 1
 number 2001
 label Sales

ephone-dn 2
 number 2002
 label Engineering
```

Phone Header Bar Display: Example

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
```

System Text Message Display: Example

The following example specifies text that should display on IP phones when they are not in use:

```
telephony-service
 system message ABC Company
```

System File Display: Example

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
```

URL Provisioning for Directories, Services, and Messages Buttons: Example

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
```

Programmable VendorConfig Parameters: Example

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 daysBacklightNotActive 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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Cisco Unified IP Phone Options

Table 62 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 62 lists the 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.

Table 62 Feature Information for Cisco Unified IP Phone Options

Feature Name	Cisco Unified CME Version	Feature Information
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.
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	3.4	Added support for provisioning customized URLs for feature buttons on supported SIP phones.
	2.0	Provisioning customized URLs for feature buttons was introduced.

Configuring Interoperability with External Services

Last Updated: July 5, 2007
First published: June 18, 2007

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 (Unified CCX).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for Interoperability Feature" section on page 987.

Contents

Information About Interoperability with External Services

To configure interoperability, you should understand the following concepts:

- Interoperability with Unified CCX, page 966

Interoperability with Unified CCX

Cisco Unified CME 4.2 and Cisco IOS Release 12.4(11)XW2 and later versions supports interoperability between Cisco Unified CME and Cisco Customer Response Solutions (CRS) 5.0 and later versions with Cisco Unified Call Center Express (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 Unified CCX application uses the CRS platform to provide a multimedia (voice, data, and web). Cisco IP IVR functionality is available with 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 Unified CCX Cisco Agent Desktop for use with Cisco Unified CME
- Configuration query and update between Unified CCX and Cisco Unified CME.
- SIP-based simple and supplementary call control services including:
  - Call routing between Cisco Unified CME and 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
- Unified CCX session management of Cisco Unified CME
- Unified CCX device and call monitoring of agent lines and call activities in Cisco Unified CME

Provisioning and configuration information in Unified CCX is automatically provided to Cisco United CME. If the configuration from 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 Unified CCX through the route point. The call is placed in a queue and redirected to the most suitable agent by Unified CCX.

Supplementary services such as call hold, blind transfer, and semi-attended transfer are initiated by Unified CCX. Existing SIP-based simple and supplementary service call flow applies except for blind transfers. For blind transfers with Unified CCX as the transferrer, 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 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 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.

Table 63 contains a list of tasks required to enable operability between Cisco Unified CME and 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 the "How to Configure Interoperability with External Services" section on page 967.

Table 63 Tasks to Configure Interoperability between Cisco CRS and Cisco Unified CME

Step	Task	Name of Document
1	Verify that Cisco Unified Communications Manager Express (Cisco Unified CME) 4.2 or a later version is installed on the router.	—
2	Configure the Cisco Unified CME router. **Tip** Note the AXL user ID, password, and router's IP address.	Prerequisites, page 968
3	Configure Cisco Unified CME to enable interoperability with Unified CCX.	How to Configure Interoperability with External Services, page 967
4	Install Cisco Unified Contact Center Express (Unified CCX) for Cisco Unified CME.	*Cisco CRS Installation Guide* at http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html.
5	Perform the initial setup of Cisco CRS for Cisco Unified CME. **Tip** When setup launches, you are asked for the AXL user ID and password that you created in Cisco Unified CME. You also need to enter the router IP address.	
6	Configure CME Telephony Subsystem to enable interoperability with Unified CCX.	*Cisco CRS Administration Guide* at http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.
7	Create users and assign the agent capability in Cisco CRS.	

How to Configure Interoperability with External Services

This section contains the following procedures:

- Configuring Cisco Unified CME to Enable Interoperability with Unified CCX, page 968 (required)
- Identifying Agent Directory Numbers in Cisco Unified CME for Session Manager, page 970 (required)
- Verifying Registrations and Subscriptions in Cisco Unified CME, page 972 (optional)
- Re-creating a Session Manager in Cisco Unified CME, page 972 (optional)
- Reconfiguring a Cisco CRS Route Point as a SIP Endpoint in Cisco Unified CME, page 974 (optional)

Configuring Cisco Unified CME to Enable Interoperability with Unified CCX

To configure Cisco Unified CME to enable interoperability between Cisco Unified CME and Unified CCX, perform the following steps.

Note A single Cisco Unified CME can support multiple session managers.

Prerequisites

- Cisco Unified CME 4.2 or a later version
- Cisco IOS Release 12.4(11)XW2 or a later version
- XML API must be configured to create a username for Unified CCX access. For configuration information, see "Configuring the XML API" on page 1005. Make note of the user ID, password, and router's IP address for using during the initial setup of Cisco CRS for Cisco Unified CME.
- Phones to be connected in Cisco Unified CME must be configured. When configuring a 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 "Configuring Conferencing" on page 665.
- The Cisco Unified CME router must be configured to accept incoming presence requests. For configuration information, see "Configuring Presence Service" on page 813.

Restrictions

- Interoperability between Cisco Unified CME and Unified CCX is restricted to one Unified CCX per Cisco Unified CME.
- Maximum number of *active* Unified CCX agents supported: 50.
- Support for Multi-Party Ad Hoc and Meet-Me Conferencing features is not provided.
- Only incoming calls from PSTN trunk are supported for deployment of the interoperability feature. Other trunks, such as SIP and H.323, are supported as usual in Cisco Unified CME, however, not for customer calls to Unified CCX.

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 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 Unified CCX for tracking call.
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.

	Command or Action	Purpose
Step 10	**sip** **Example:** `Router(config-voi-srv)# 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. • **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.

Identifying Agent Directory Numbers in Cisco Unified CME for Session Manager

To specify which directory numbers, associated with phone lines on Unified CCX agent phones, can be managed by a session manager, perform the following steps.

Prerequisites

- Up to eight session managers must be configured in Cisco Unified CME.
- Directory numbers associated with Unified CCX agent phones must be configured. 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. For configuration information, see "Configuring Phones to Make Basic Calls" on page 165.

Restrictions

- 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 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 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.
- For call forward and call pickup, the directory number of an agent cannot forward to a Cisco CRS route point.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn** *dn-tag*
4. **allow watch**
5. **session-server** {*session-tag*[**,...***session-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	**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 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 5	**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 6	**end** **Example:** `Router(config-ephone-dn)# end`	Exits configuration mode and enters privileged EXEC mode.

Verifying Registrations and Subscriptions in Cisco Unified CME

Before using the system, verify registrations and subscriptions for 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 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-creating a Session Manager in Cisco Unified CME

Note Provisioning and configuration information in Unified CCX is automatically provided to Cisco United CME. The following task is required only if the configuration from Unified CCX is deleted or must be modified.

To re-create a session manager in Cisco Unified CME for 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 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 Unified CCX is deleted or must be modified. • *name*—String for identifying 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 Unified CCX is deleted or must be modified. • Keepalive duration for registration, in seconds, after which the registration expires unless Unified CCX reregisters before the registration expiry. • Range: 60 to 3600. Default: 300. **Note** Default in Unified CCX is 120.
Step 6	**end** **Example:** `Router(config-register-fs)# end`	Exits configuration mode and enters privileged EXEC mode.

Reconfiguring a Cisco CRS Route Point as a SIP Endpoint in Cisco Unified CME

Note Provisioning and configuration information in Unified CCX is automatically provided to Cisco United CME. The following task is required only if the configuration from 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.

Prerequisites

- 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 "Configuring Phones to Make Basic Calls" on page 165.
- Directory numbers associated with Cisco CRS route points must be enabled to be watched. For configuration information, see "Configuring Presence Service" on page 813.
- The **mode cme** command must be enabled in Cisco Unified CME.

Restrictions

- 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register dn** dn-tag
4. **number** *number*
5. **allow watch**
6. **refer target dial-peer**
7. **exit**
8. **voice register pool** *pool-tag*
9. **number** *tag* **dn** *dn-tag*
10. **session-server** *session-tag*
11. **codec** *codec-type* [*bytes*]
12. **dtmf-relay rtp-relay sip-notify**
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	**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	**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 6	**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 7	**exit** **Example:** `Router(config-register-dn)# exit`	Exits configuration mode to the next highest mode in the configuration mode hierarchy.
Step 8	**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 Unified CCX can contain up to 10 individual SIP endpoints. Subsequent pools are created for additional SIP endpoints.
Step 9	**number** *tag* **dn** *dn-tag* **Example:** `Router(config-register-pool)# number 1 dn 1`	Associates a directory number with the route point being configured.

	Command or Action	Purpose
Step 10	**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.
Step 11	**codec g711ulaw** **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 Unified CCX.
Step 12	**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 13	**end** **Example:** `Router(config-register-pool)# end`	Exits configuration mode and enters privileged EXEC mode.

Configuration Examples for Interoperability with Unified CCX

The following output from the **show running-configuration** command shows the configuration on a Cisco Unified CME router that will interoperate with 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&m-immediate-start
!
controller T1 0/3/1
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 0 timeslots 1-4 type e&m-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
 max-ephones 240
 max-dn 720
 ip source-address 192.0.2.254 port 2000
 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 "Generating Configuration Files for Phones" on page 265.

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	• *Cisco Unified CME Command Reference* • *Cisco Unified CME* documentation roadmap
Cisco Unified Contact Center Express (Unified CCX)	• *Cisco Unified Contact Center Express* documentation road map
Cisco Customer Response Solutions (CRS)	• *Cisco CRS Installation Guide* • *Cisco CRS Administration Guide*
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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Interoperability with External Services

Table 64 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified Communications Manager Express and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 64 lists the 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.

Table 64 Feature Information for Interoperability Feature

Feature Name	Cisco Unified CME Version	Modification
Interoperability with External Services	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 (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.

Configuring SRST Fallback Support

Last Updated: March 26, 2007

This chapter describes SRST fallback support using Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for SRST Fallback Support" section on page 1003.

Contents

Prerequisites for SRST Fallback Support

- 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.
- Tasks in "Generating Configuration Files for Phones" on page 265 must be completed.
- Tasks in "Configuring System-Level Parameters" on page 137 must be completed.
- Tasks in "Generating Configuration Files for Phones" on page 265 must be completed.
- Tasks in "Configuring Call Transfer and Forwarding" on page 517 must be completed.

Restrictions for SRST Fallback Support

- 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 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 chassis. 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_documentation_roadmap09186a0080189132.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 purely random.

Information About SRST Fallback Support

To configure SRST fallback support, you should understand the following concepts:

- SRST Fallback Support Using Cisco Unified CME, page 990
- Prebuilding Cisco Unified CME Phone Configurations, page 994

SRST Fallback Support 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 the Cisco Unified CME router in SRST 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

5. 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."
6. 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
7. 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.
8. 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.
9. 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.

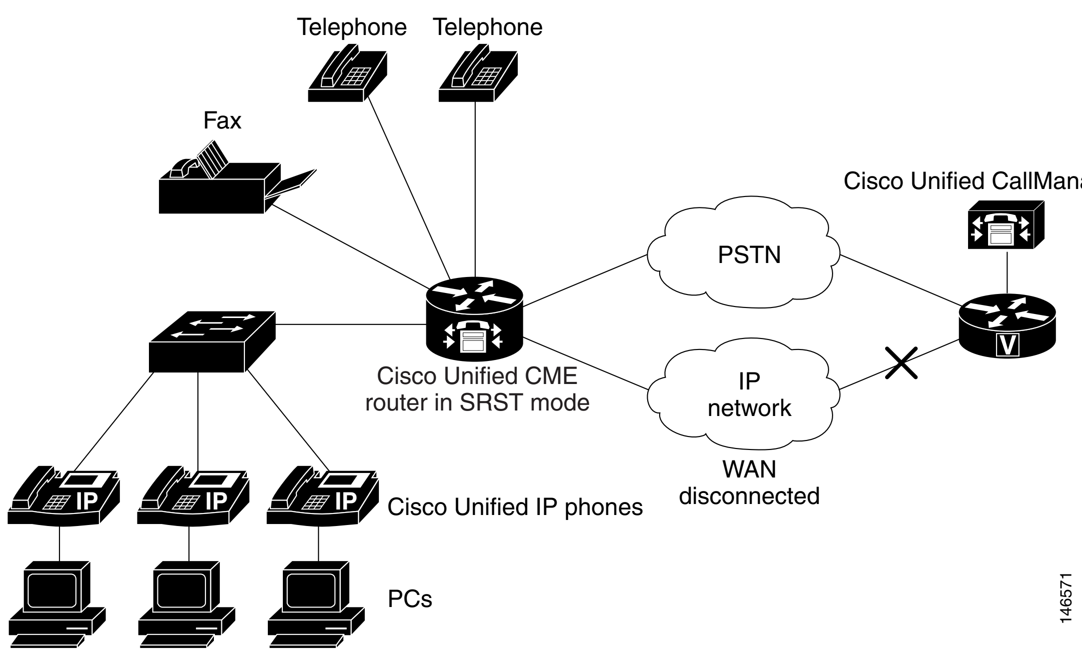
A Cisco Unified IP phone will not reestablish a connection with the primary Cisco Unified Communications Manager at the central office if it is engaged in an active call.

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 53 shows a branch office with several Cisco Unified IP phones connected to a Cisco Unified CME router in SRST 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 53 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 47.

How to Configure SRST Fallback Support

This section contains the following tasks:

- Enabling SRST Mode, page 994 (required)
- Verifying SRST Mode, page 996 (optional)
- Prebuilding Cisco Unified CME Phone Configurations, page 997 (optional)
- Modifying Call Pickup for Fallback Support, page 997 (optional)

Enabling SRST Mode

To enable SRST mode on the Cisco Unified CME router, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **srst mode auto-provision** {**all** | **dn** | **none**}
5. **srst dn line-mode** {**dual** | **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** | **single**} **Example:** `Router(config-telephony)# srst dn line-mode dual`	(Optional) Specifies the line mode for ephone-dns in SRST mode on a Cisco Unified CME router. • **dual**—SRST fallback ephone-dns will be dual-line ephone-dns. • **single**—SRST fallback ephone-dns will be single-line ephone-dns. **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.
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 "Configuring Templates for Fallback Support: Example" on page 1000. • *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.

	Command or Action	Purpose
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.

Verifying SRST Mode

Step 1 Use the **show telephony-service all** or the **show running-config** command to verify that SRST mode has been set on this router.

```
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
 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.

```
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.

```
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.

See the following procedures to set up a few of the most common features to associate with phones in fallback mode:

- "SCCP: Creating Directory Numbers" section on page 177
- "Enabling Call Park" section on page 508
- "SCCP: Enabling Ephone Templates" section on page 929
- "SCCP: Enabling Ephone-dn Templates" section on page 930
- "SCCP: Configuring Hunt Groups" section on page 614

Modifying 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.
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 Support

This section contains the following examples:

Enabling SRST Mode: Example

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
 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
```

Provisioning Directory Numbers for Fallback Support: Example

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
```

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 soft-key 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
```

Enabling Hunt Groups for Fallback Support: Example

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
```

Modifying Call Pickup for Fallback Support: Example

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
```

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for SRST Fallback Support

Table 65 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 65 lists the 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.

Table 65 Feature Information for SRST Fallback Support

Feature Name	Cisco Unified CME Version	Feature Information
SRST Fallback Support Using Cisco Unified CME	4.0	SRST fallback support using Cisco Unified CME was introduced.

Configuring the XML API

Last Updated: March 26, 2007

This chapter describes the eXtensible Markup Language (XML) Application Programming Interface (API) support available in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco Unified CME version may not support all of the features documented in this module. For a list of the versions in which each feature is supported, see the "Feature Information for XML API" section on page 1014.

Contents

Information About XML API

To enable XML API, you should understand the following concepts:

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.

How to Configure XML API

This section contains the following tasks:

Note The following Cisco IOS commands that were previously used with the XML interface are no longer valid: **log password**, **xmltest**, **xmlschema**, and **xmlthread**.

Defining 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.
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.

Defining 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`	Specifies the Cisco Unified CME application and enters XML-application configuration mode.
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.

Defining 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*—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.

Defining 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

Step 1 Use the **debug cme-xml** command to view debug messages for the Cisco Unified CME XML interface.

Configuration Examples for XML API

This section contains the following examples:

XML Transport Parameters: Example

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
```

XML Application Parameters: Example

The following example sets the application response timeout to 30 seconds.

```
ixi application cme
 response timeout 30
 no shutdown
```

XML Authentication: Example

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
```

XML Event Table: Example

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

Additional References

The following sections provide references related to Cisco Unified CME features.

Related Documents

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*
Phone documentation for Cisco Unified CME	• Quick Reference Cards • User Guides

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for XML API

Table 66 lists the features in this module and enhancements to the features by version.

To determine the correct Cisco IOS release to support a specific Cisco Unified CME version, see the *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix* at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 66 lists the 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.

Table 66 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.

INDEX

Numerics

A

B

C

D

E

F

G

H

O

P

S

T

U

V

W

X