



Cisco CallManager Express (CME) 3.0 Design Guide

This design guide provides Cisco system engineers, partners, and customers with a series of guidelines and best practices to deploy Cisco CME 3.0, formerly known as Cisco IOS Telephony Services (ITS), as a standalone router in small/branch offices, to add a Cisco CME (CME) router to an H.323 network with call transfer/forward support in H.450, to add a Cisco CME router in a Session Initiation Protocol (SIP) network, and so forth. This document covers the system requirements and specifications for Cisco CME 3.0, deployment scenarios, and design considerations for the call transfer/forward, voice-mail integration options, network management capabilities, Cisco CME with Network Address Translation (NAT), and firewalls. It also includes troubleshooting commands and Cisco CME known issues and caveats.

Contents

- [About Cisco CME, page 2](#)
- [Deployment Scenarios and Design Considerations, page 13](#)
- [Voice Mail, page 26](#)
- [Provisioning and Network Management for Cisco CME, page 42](#)
- [AA with TCL and VxML, page 48](#)
- [Cisco CME with NAT/Cisco IOS Firewall, page 51](#)
- [Troubleshooting Cisco CME Features, page 53](#)
- [Additional References, page 55](#)
- [Appendix: XML Test Program APIs, page 57](#)



About Cisco CME

This section contains overview information about Cisco CME that includes the following:

- [Cisco CME 3.0 Features, page 3](#)
- [Hardware and Software System Requirements, page 6](#)
- [Cisco CME Licenses, page 11](#)
- [Cisco CME 3.0 Installation, page 12](#)
- [Cisco CME Upgrade from Version 2.1 to Version 3.0, page 13](#)

Cisco CME is an optional Cisco IOS software feature that enables Cisco routers to deliver key system or hybrid PBX functionality for enterprise branch offices or small businesses. Cisco CME is ideal for customers for data connectivity requirements that also have a need for a telephony solution for that office. Whether offered through a service provider's managed services, or purchased directly by a corporation, Cisco CME offers many of the core telephony features required in the small office and many advanced features not available on traditional telephony solutions. Being able to deliver IP telephony and data routing on a single converged solution allows customers to optimize their operations and maintenance costs, resulting in a very cost effective solution to meet the office needs.

Cisco CME supports all the existing features in Cisco IOS routers acting as voice gateways. In addition, the Cisco CME provides the call processing capability for supporting up to 120 users by using the Skinny Client Control Protocol (SCCP). The Cisco CME supports the Cisco 7902, Cisco 7905G, Cisco 7910, Cisco 7912G, Cisco 7914 Expansion Module, Cisco 7920, Cisco 7935 polycom, Cisco 7940, and Cisco 7960, and can be integrated with the ATA 186/188 with two analog phone endpoints for cost effective SCCP-based call processing. The router first loads IP phone images to the phones and configures and manages the IP phones. Cisco CME also provides capabilities for call forward and call transfer to other phone numbers or devices such as voice-mail systems. Cisco CME routers are mainly deployed in the two scenarios shown in [Figure 1](#) and [Figure 2](#).

Figure 1 *Deploying of Cisco CME in a Small Medium Business (SMB) or Small Enterprise Offices (Retail Stores)*

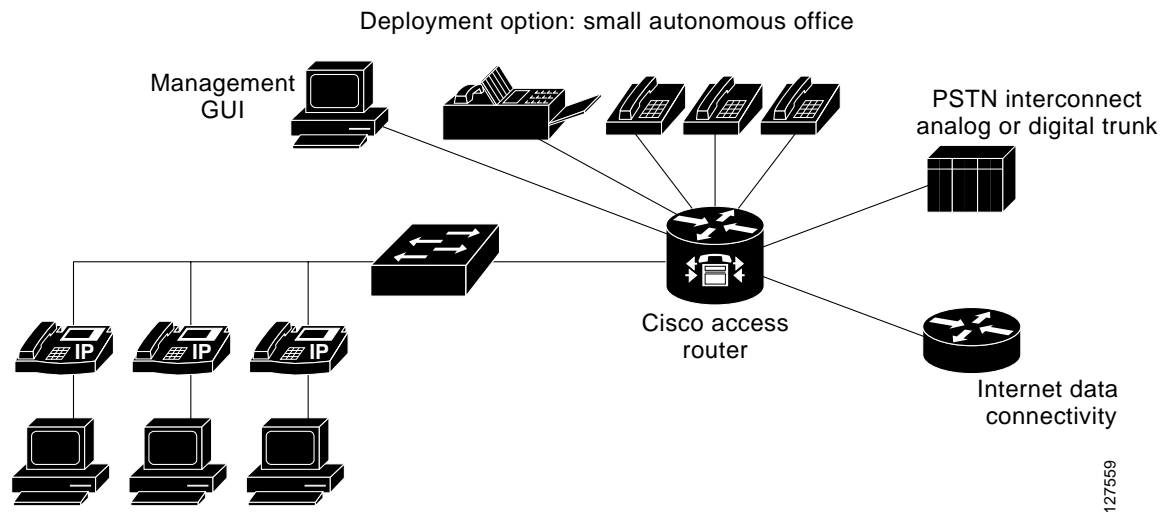
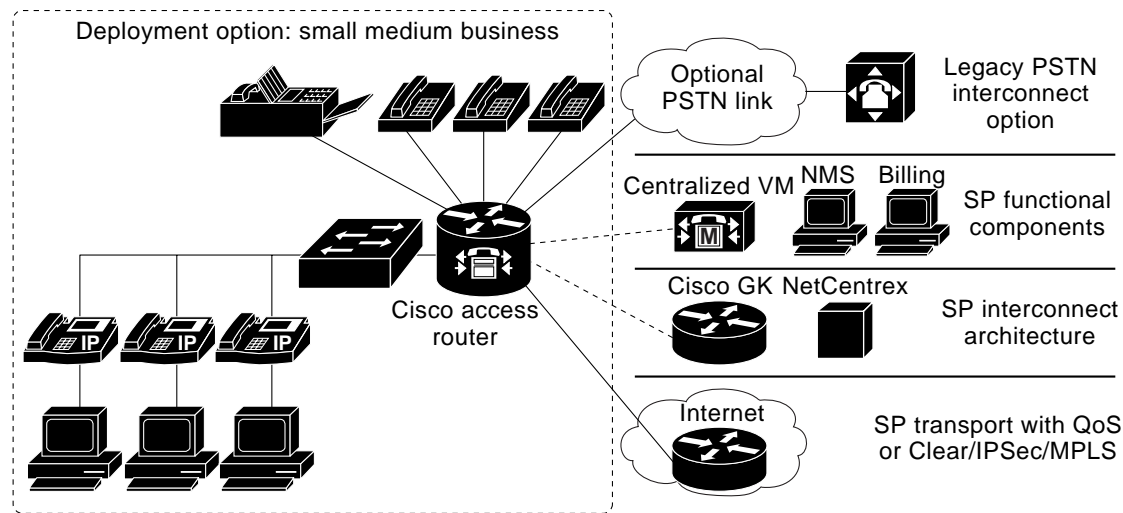


Figure 2 *Deploying Cisco CME in a Small Medium Business (Cisco 7905G) Offered Through a Service Provider Managed Service*



Cisco CME 3.0 Features

Cisco CME 3.0 is available in Cisco IOS Release 12.2(15)ZJ and has the following new features since the Cisco CME 2.1 release. Note that the latest software with 120 phone support is in Cisco IOS Release 12.2(15)ZJ3.

Phone Features

- Cisco IP phone 7902, IP phone 7905G, IP phone 7912G, and Cisco 7920 IP phone support
- Attendant console functionality using the Cisco IP Phone 7960 and Cisco IP Phone 7914 Expansion Modules—fast transfer, busy lamp field, and direct station select
- Silent and feature ringing options
- Do Not Disturb soft key
- Speed-dial configuration from IP phone
- Fast-dial support
- Label support
- Call Fwd All soft key on IP phone
- Silent and feature-ring options
- European date formats
- Dual-line mode for call waiting, call conferencing, and call transfer features support
- Flash soft key for hookflash functionality for the PSTN
- Phone directory entry

Manageability Improvements

- Automatic assignment of free extension numbers to new IP phones
- Telephony service configuration wizard
- Cisco CME setup for quick installation
- Cisco CME GUI enhancements and customization
- Syslog message support for phone registration/deregistration
- Account codes support/display in call detail record (CDR)
- Cisco AVVID XML Layer (AXL) and Simple Object Access Protocol (SOAP) capabilities for configuration changes
- Service provider class network management

System Features

- Additional language support—Portuguese, Dutch, Danish, Norwegian, and Swedish
- Night service bell
- Call pickup explicit ringing extension
- Call pickup local group ringing phone
- Call pickup explicit group ringing phone
- Hunt groups—sequential, random, and parallel
- Secondary dial tone
- Call back busy subscriber/camp-on
- Call blocking (toll bar) based on time of day, day of week, or date
- Call blocking (toll bar) override/self-login
- Per-call caller ID blocking
- Extension overlays for better call handling and distribution

Trunk Features

- E1 R2 support
- SIP trunk support



Note

Cisco CME 3.0 also supports all the other features introduced in Cisco CME 1.0, 2.0, and 2.1.

Cisco CME 1.0 Features

- Dial-plan class of restriction (COR)
- Call hold and retrieve
- Call pickup of on-hold calls
- Multiple lines per Cisco IP phone (up to 6 lines per phone)
- Multiple line appearance across telephones (up to 24)
- Call forwarding functions—all, busy, and no answer
- Call transferring
- Speed dialing

- Cisco IP phones derive the date and time from the router through Network Time Protocol (NTP)
- Interworking with Cisco gatekeeper
- Distinctive ringing—external ringing versus internal ringing
- Caller identification display and blocking
- Analog Foreign Exchange Station (FXS) and Foreign Exchange Office (FXO) ports
- On-net calls using VoIP H.323, VoFR, and VoATM

Cisco CME 2.0 Features

- Conference
- Paging
- Intercom
- Basic automated attendant using TCL 2.0
- GUI for simple moves, adds, and changes
- Local directory support
- Timeout alert
- Tone on hold, tone on transfer, music on hold (MOH), music on transfer
- Primary Rate Interface support (N/A to Cisco 1751)
- H.323 transfer across Cisco IOS endpoints
- Alias lists
- Translation rules
- Class of restriction (COR)
- Distinctive ringing
- Cisco IP Phone 7910 support—two lines per button
- Cisco Unity (Active Voice) voice-mail integration
- Dual tone multifrequency (DTMF) based voice-mail integration (Active Voice—Reception product)
- Interactive voice response (IVR) functionality using Tool Command Language (Tcl) 2.0
- SIP message-waiting indication (MWI) and MWI directory number (DN) for centralized voice-mail service
- Extensible Markup Language (XML) services
- Loopback-dn support for call transfer and call forward support on Cisco and third-party gateways—12-hour and 24-hour mm-dd-yy and dd-mm-yy formats for time and date

Cisco CME 2.1 Features

- Consultative transfer
- H.450.2 and H.240.3 for call transfer and redirect
- Hookflash transfer support for analog phones
- International language support—German, French, Italian, and Spanish
- Top line (phone display) text description
- XML based local speed dials

- XML phone load support
- MOH live feed
- GUI customization feature
- Support for the Cisco IP Phone 7914 Expansion Module
- ATA 186/188, introduced in Cisco IOS Release 12.2(11)T
- Global call forward enhancement
- Enhanced **dial-plan pattern** command
- Cisco Unity (Active Voice) voice-mail integration
- Oh-hook dialing (phone feature)
- System speed-dial option through XML service
- Silent ring on shared line—use with Cisco IP Phone 7960 and Cisco IP Phone 7914 Expansion Modules to provide Auto Attendant (AA) support
- Idle URL—ability to push specific messages onto the screen of a Cisco IP Phone 7940 or Cisco IP Phone 7960 phone on a periodic basis

Hardware and Software System Requirements

This section includes information about the following:

- [Supported Platforms, IP Phones, DN, and Memory Requirements, page 6](#)
- [Memory Requirements, page 8](#)
- [Cisco IOS Images, Cisco CME Releases, and Cisco CME Files, page 9](#)
- [Supported IP Phones and Phone Loads, page 10](#)

Supported Platforms, IP Phones, DN, and Memory Requirements

Cisco CME uses the terms *ephone*, *ephone-dn*, and *virtual voice ports* for IP phones. A virtual voice port is similar to a physical voice port, but it is not tied with physical resources. Virtual voice ports can be considered as “lines” to allow multiple lines per physical IP phone. A virtual voice port is equivalent to the IP phone extension and ephone directory number (ephone-dn). Ephone-dns or virtual voice ports are used for line appearances, intercom, paging, conferencing, voice-mail pilot number, voice-mail ports, and voice-mail MWI. Cisco CME automatically creates a POTS dial peer when each ephone-dn is configured. If an ephone-dn is configured with a secondary number as below, Cisco CME will create two POTS dial peers, one for 0100, and another for 408-555-0100:

```
ephone-dn 1
  number 0100 secondary 408-555-0100
```

While continuing support of most of the platforms supported in Cisco CME 2.1, Cisco CME 3.0 adds support for the Cisco IAD 243x series, 1760-V, and Cisco Catalyst 4500 AGM. Note that Cisco CME 3.0 is not supported on the Cisco IAD 2420 series, Cisco 3620, and Cisco 2600 series (non-XM series). [Table 1](#) shows IP phone, DN, and memory requirements for all supported platforms with Cisco IOS Release 12.2(15)ZJ3.



Note

Because analog phones connected to the FXS ports of the Cisco IAD 243x are locally controlled and not under SCCP control, they do not support Cisco CME features.

Table 1 Cisco CME in 12.2(15)ZJ3

Platform	Phones	Virtual Voice Ports	IP Plus (is)		Enterprise Basic (jls3)		Enterprise Plus (js)	
			Min	Rec ¹	Min	Rec ¹	Min	Rec ¹
IAD2420	—	—	—	—	—	—	—	—
IAD 2430-24FXS	24	120	32/64	32/96	32/64	32/96	32/64	32/96
IAD 2431-1T1E1	24	120	32/64	32/96	32/64	32/96	32/64	32/96
IAD 2431-8FXS	24	120	32/64	32/96	32/64	32/96	32/64	32/96
IAD 2431-16FXS	24	120	32/64	32/96	32/64	32/96	32/64	32/96
IAD 2431-24FXS	24	120	32/64	32/96	32/64	32/96	32/64	32/96
1751 ²	24	120	16/64	16/96	—	—	—	—
1751-V ²	24	120	32/96	32/96	—	—	—	—
1760/1760-V ²	24	120	32/96	32/96	—	—	—	—
2600 classic/3620	—	—	—	—	—	—	—	—
261xXM	36	144	32/96	32/128	—	—	32/96	32/128
262xXM	36	144	32/96	32/128	—	—	32/96	32/128
265xXM	48	192	32/96	32/128	—	—	32/96	32/128
2691	72	432	32/128	32/128	—	—	32/128	32/128
3640/3640A	48	288	32/96	32/128	—	—	32/96	32/128
3660	96	576	32/96	32/128	—	—	32/96	32/128
3725	96	576	32/128	32/128	—	—	32/128	32/128
3745	120	720	32/128	32/128	—	—	32/128	32/128
Cisco Catalyst 4500 AGM ³	24	48	32/64	32/64	32/64	32/64	32/64	32/64
Cisco Catalyst 4500 AGM ³	96	576	32/128	32/128	32/128	32/128	32/128	32/128

1. Recommended flash memory/DRAM ready for the next mainline release.
2. Cisco CME is available only with Cisco IOS release IP/VOX PLUS images for the 1751-V and 1760/1760-V Cisco CME with 1751 is available only with the IP/VOX PLUS sv8y image.
3. These are the same model, but each supports a different number of IP phones and DNs based on the amount of memory available on the system. Support on the Cisco Catalyst 4500 AGM will not be in 12.2(15)ZJ, but in 12.3(4)T.

Table 2 shows IP phone, DN, and memory requirements for all supported platforms with Cisco IOS Release 12.2(15)ZJ.

Table 2 Cisco CME in 12.2(15)ZJ3

Platform	Phones	Virtual Voice Ports	IP Plus (is)		Enterprise Basic (jls3)		Enterprise Plus (js)	
			Min	Rec ¹	Min	Rec ¹	Min	Rec ¹
IAD2420	—	—	—	—	—	—	—	—
IAD 243x	24	120	32/64	32/96	32/64	32/96	32/64	32/96
1751	24	120	16/96	16/96	—	—	—	—

Table 2 Cisco CME in 12.2(15)ZJ3 (Continued)

Platform	Phones	Virtual Voice Ports	IP Plus (is)		Enterprise Basic (jls3)		Enterprise Plus (js)	
			Min	Rec ¹	Min	Rec ¹	Min	Rec ¹
1751-V	24	120	32/96	32/96	—	—	—	—
1760/1760-V	24	120	32/96	32/96	—	—	—	—
2600XM	24	120	32/96	32/128	—	—	32/96	32/128
265x	—	—	—	—	—	—	—	—
265xXM	48	192	32/96	32/128	—	—	32/96	32/128
2691	48	288	32/128	32/128	—	—	32/128	32/128
3640/3640A	48	288	32/96	32/128	—	—	32/96	32/128
3660	48	288	32/96	32/128	—	—	32/96	32/128
3725	48	288	32/128	32/128	—	—	32/128	32/128
3745	48	288	32/128	32/128	—	—	32/128	32/128
2600 classic/3620	—	—	—	—	—	—	—	—
Cat 4500 AGM ²	24	48	32/64	32/64	32/64	32/64	32/64	32/64
Cat 4500 AGM ²	48	192	32/128	32/128	32/128	32/128	32/128	32/128

1. Recommended flash memory/DRAM ready for the next mainline release.
2. These are the same model, but each supports a different number of IP phones and DN's based on the amount of memory available on the system. Support on the Cisco Catalyst 4500 AGM will not be in 12.2(15)ZJ, but in 12.3(4)T.

Memory Requirements

Each dial peer requires approximately 35 KB, or 50 to be more conservative. [Table 3](#) shows the memory calculation based on 48, 120, 192 DN's and each DN requires about 50k bytes.

Table 3 Memory Per Ephone and Number of DN's

Ephone	DN's	Required Memory (KB)
24	120	6,000
36	144	7,200
48	288	14,400
120	432	21,600
192	576	28,800
288	720	36,000

Memory requirement is not based only on the amount required for all the ephone-dns; it also depends on the router's configuration, features, routing protocols, processes, traffic types, and so on. In addition, the Cisco CME router will always need to keep some space for other processes to prevent further ephone-dns from being created if the router's memory is below some certain limit.

Minimum memory is the amount needed to load the Cisco IOS Cisco CME image; the recommended memory is what is needed to run all the features with traffic. Flash memory and DRAM requirements are not only dependent on Cisco CME increased features, but also on the image size and other features in Cisco IOS routers when Cisco CME software is merged with the T train or mainline images.

As always, the more features are added, the more memory is needed. In addition to the minimum memory requirement, we encourage customers to get more memory up front if the router is fully loaded and configured with a lot of features, protocols, and traffic.

Cisco IOS Images, Cisco CME Releases, and Cisco CME Files

Cisco 2600, Cisco 3600, and Cisco 3700 series running Cisco CME 3.0 require a minimum of an IP Plus image. The Cisco 1751 and Cisco 1760 series require a VOX PLUS image or greater. All systems require CME files that shipped are with Cisco CME and copied to the flash memory of the router. Cisco CME 3.0 files can be downloaded from CCO as well.

Cisco CME files can be copied individually or in bulk from the following CCO download pages:

- <http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key>
- <http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp>

The following is list of files contained in cme-gui-3.0.3.tar, cme-basic-3.0.3.tar, and cme-3.0.3.zip/tar:



Note

cme-gui-3.0.3.tar contains all the GUI and xml.template files.

- CiscoLogo.gif
- dom.js
- normal_user.js
- Delete.gif down
- arrow.gif
- sxiconad.gif
- Plus.gif
- ephone_admin.html
- telephony_service.html
- Tab.gif
- its-gui-3.0.2.tar
- uparrow.gif
- admin_user.html
- logohome.gif
- xml-test.html
- admin_user.js
- normal_user.html
- xml.template

The following is a list of files contained in cme-basic-3.0.3.tar:

- CP79020101SCCP030530B.sbin
- cmterm_7920.3.3-01-02-021.bin
- CP79050101SCCP030530B.sbin
- CP79120101SCCP030530B.sbin

- its-CISCO.2.0.1.0.tcl
- P00303020214.bin
- P00403020214.bin
- cme-gui-3.0.3.tar
- S00103020002.bin
- music-on-hold.au
- ata18x-v2-16-ms-030327b.zup

The following is a list of files contained in cme-3.0.3.zip/tar:

- cme-basic-3.0.3.tar
- app-h450-transfer.2.0.0.7.zip (H.450 call transfer script for analog phones connected to FXS ports)
- CiscoIOSTSP.zip (TSP file for TAPI light support)

Table 4 shows a list of information for Cisco IOS images and Cisco CME files.



Note

Cisco CME 3.0 files are not compatible with Cisco CME 2.1 or Cisco CME 2.0 files. The following is a list of information for Cisco IOS images and Cisco CME files.

Table 4 Cisco IOS Images and Cisco CME Files

Cisco CME Version	Cisco CME File	Cisco IOS Release
Cisco CME 3.0	cme-3.0.3.zip/tar	12.2(15)ZJ3
	cme-basic-3.0.3.tar	12.3(4)T
Cisco CME 2.1	its-2.1.0.4.zip	12.2(11)YT
		12.2(15)T /w IDS/FW/IPSec
Cisco CME 2.0	CME-2.0.zip	12.2(8)T5
		12.2(11)T
		12.2(13)T

Supported IP Phones and Phone Loads

Cisco CME allows the Cisco CME router to plug and unplug the Cisco IP phones without requiring a router reboot or manual status reset. If the Cisco CME router is configured properly and has required phone loads in flash memory, IP phone registration with the Cisco CME router is an automatic process. When powered on or connected to the Cisco CME router, the IP phone sends a DHCP client request to Cisco CME for an IP address, IP phone load/firmware, and phone configuration details. As a DHCP and TFTP server, Cisco CME responds with an IP address and phone load and configures the IP phone according to the configuration entered in the router.

The new IP phones supported in Cisco CME 3.0 are the Cisco 7902, 7905G, and 7912G IP phones. Support for Cisco IP Phone 7920 will be added in a later release.

Table 5 shows all the phones and phone loads supported in Cisco CME releases.

Table 5 Phone Loads

Phone Type	Phone Loads		
	Cisco CME 2.0	Cisco CME 2.1	Cisco CME 3.0
Cisco ATA 186/188	—	ata18x-v2-15-ms-020927a.zup	ata18x-v2-16-ms-030327b.zup
Cisco 7902G	—	—	CP79020101SCCP030326A.SBIN
Cisco 7905G	—	—	CP79050101SCCP030404A.SBIN
Cisco 7910	P004G302	P00403020209	P00403020214
Cisco 7912G	—	—	CP79120101SCCP030404A.SBIN
Cisco 7914 Expansion Module	—	S00103020002	S00103020002
Cisco7920	—	—	cmterm_7920.3.3-01-02-021.bin
Cisco 7935 polycom	—	P00503010100	P00503010100
Cisco 7940	P003G302	P00303020209	P00303020214
Cisco 7960	P003G302	P00303020209	P00303020214

Cisco CME Licenses

You must purchase a Cisco CME feature license and phone seat licenses (also called user licenses) prior to using the Cisco CME feature in any production network. [Table 6](#) and [Table 7](#) list platforms and IP phones supported by Cisco CME 3.0 and their part numbers.

Table 6 Platform and Number of Phones Supported by Cisco CME 3.0 and Platform Part Number

Platform	Phones Supported	Part Number	Spare Part Number
Cisco 1751-V, Cisco 1760/1760-V, and Cisco IAD 243x	Up to 24 phones	FL-CCME-SMALL	FL-CCME-SMALL=
Cisco 261x and Cisco 262x(XM)	Up to 36 phones	FL-CCME-36NTE	FL-CME-36NTE=
Cisco 265x(XM)	Up to 48 phones	FL-CCME-MEDIUM	FL-CCME-MEDIUM=
Cisco 2691	Up to 72 phones	FL-CCME-UL-72	FL-CCME-UL-72=
Cisco 3725	Up to 96 phone	FL-CCME-UL-96	FL-CCME-UL-96=
Cisco 3660 and Cisco 3745	Up to 120 phone	FL-CCME-UL-120	FL-CCME-UL-120=

Table 7 IP Phones Supported by Cisco CME 3.0 and Their Part Number

IP Phone	Lines Supported	Part Number	Spare Part Number
Cisco ATA 186/188	single-line phone	SW-CCME-UL-ANA	SW-ITS-UL-ANA(=)
Cisco 7902	single-line phone	SW-CCME-UL-7902 SW-CCME-UL-7920	SW-ITS-UL-7902G(=) SW-ITS-UL-7920G(=)
Cisco 7905G	single-line phone	SW-CCME-UL-7905G	SW-ITS-UL-7905G(=)
Cisco 7910	single-line phone	SW-CCME-UL-7910	SW-ITS-UL-7910(=)
Cisco 7912G	single-line phone	SW-CCME-UL-7912G	SW-CCME-UL-7912G(=)

Table 7 IP Phones Supported by Cisco CME 3.0 and Their Part Number

IP Phone	Lines Supported	Part Number	Spare Part Number
Cisco 7935 polycom	multiline phone	SW-ITS-CCME-7935	SW-CCME-UL-7935(=)
Cisco 7940	multiline phone	SW-CCME-UL-7940(=)	SW-ITS-UL-7940(=)
Cisco 7960	multiline phone	SW-CCME-UL-7960(=)	SW-ITS-UL-7960(=)

**Note**

Cisco CME license and phone seat licenses can be converted to Cisco CallManager and Cisco SRST licenses without any additional cost. See the “[Cisco CME Migration to Cisco CallManager and Cisco SRST](#)” section on page 25 for more details.

Cisco CME 3.0 Installation

Before configuring Cisco CME features, make sure that you get the Cisco CME 3.0 files from CCO at <http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key> or <http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp> and then copy and extract the files onto flash memory or slot 0 of the Cisco CME router. For ease of installation, you may download the `cme-basic-3.0.3.tar` file which includes all of the supported phone loads, Cisco CME GUI files, and MOH file to install and set up supported IP phones. See the file list in the “[Cisco IOS Images, Cisco CME Releases, and Cisco CME Files](#)” section on page 9. If this is not a new installation, but an upgrade from a previous installation with a `zj1` or a `zj2` image, you must copy and install the CME GUI files (`cme-gui-3.0.3.tar`) into flash memory only, as all the supported phone loads and MOH files are already on the flash memory and are still valid for `zj3` installation.

**Note**

Cisco CME files can be copied individually or in bulk from the above CCO download page.

For advanced users, you may download only those needed files to the router’s flash memory.

The following steps allow you to extract contents of the tar file to router flash memory using the **archive** command.

Step 1 Download the appropriate tar file to the TFTP server.

- `cme-basic-x.x.x.tar`—Contains basic Cisco CME system files including GUI, MOH, and phone loads.
- `cme-gui-x.x.x.tar`—Contains basic Cisco CME GUI files only.

Step 2 Log in to privileged EXEC mode of the router CLI.

Step 3 Enter the **archive** command to extract the contents of the tar file to router flash memory:

```
Router# archive tar /xtract tftp://ip-address/filename flash:
```

- Example 1: To extract the contents of `cme-basic-3.0.3.tar` from TFTP server 192.168.1.1 to flash memory, enter the following:

```
Router# archive tar /xtract tftp://192.168.1.1/cme-basic-3.0.3.tar flash:
```

- Example 2: To extract the contents of cme-gui-3.0.3.tar from TFTP server 192.168.1.1 to flash memory, enter the following:

```
Router# archive tar /xtract tftp://192.168.1.1/cme-gui-3.0.0.tar flash:
```

Note that if you have already copied .tar file to flash memory, you should use flash memory instead of tftp://192.168.1.1.

- Step 4** Refer to the [Cisco CallManager Express 3.0 System Administrator Guide](#) on Cisco.com for Cisco CME configuration information.
-

Cisco CME Upgrade from Version 2.1 to Version 3.0

The following steps allow you to upgrade a Cisco CME router from Cisco CME 2.1 to Cisco CME 3.0.

- Step 1** Copy the Cisco CME 3.0 Cisco IOS image onto flash memory.
- Step 2** Copy Cisco CME 3.0 supported phone loads onto flash memory. See [Table 5 on page 11](#) for phone load information.

- Step 3** Configure the router. For example:

```
tftp-server flash:P00303020214.bin
tftp-server flash:P00303020214.bin
telephony-service
load 7910 P00403020214
load 7960-7940 P00303020214
```

- Step 4** Remove the H.450 call transfer script from ephone-dns and dial peers, assuming that bator is the application name used.

```
telephony-service
no application appname
application name
```

If you configured “application bator” manually for the ephone-dns, configure the following:

```
telephony-service
application appname
no application appname
```

- Step 5** Reload the router.
-

Deployment Scenarios and Design Considerations

This section provides information about the following:

- [PBX Versus Key-Switch Mode, page 14](#)
- [Standalone Cisco CME—Cisco CME with PSTN Interfaces, page 14](#)
- [Dial-Plan Management, page 16](#)
- [Call Transfer and Call Forward, page 17](#)
- [Cisco CME in SIP Networks, page 24](#)

- [Cisco CME Integration with Cisco CallManager, page 25](#)
- [Cisco CME Migration to Cisco CallManager and Cisco SRST, page 25](#)

PBX Versus Key-Switch Mode

Cisco CME can be set up or deployed as systems similar to a PBX or a key switch. If you use the Cisco CME setup tool, you will be asked to choose PBX or key-switch mode so that the Cisco CME setup tool will install one button per call or two calls per button on the IP phones, respectively. Both PBX and key-switch modes can be mixed and combined on the same types of the phones.

Cisco CME in PBX Mode

IP phones have only one line displayed on a single button, and each button is associated with two channels to support call waiting, call transfer, and conference. You will usually select PBX mode for Cisco IP Phone 7905G or Cisco IP Phone 7910. The following features can be used for, but are not limited to, the PBX mode:

- XML service
- IVR AA
- Cisco Unity Express voice mail
- Cisco IP Phone 7902, Cisco IP Phone 7905G, Cisco IP Phone 7910, Cisco IP Phone 7912G

Cisco CME in Key Switch Mode

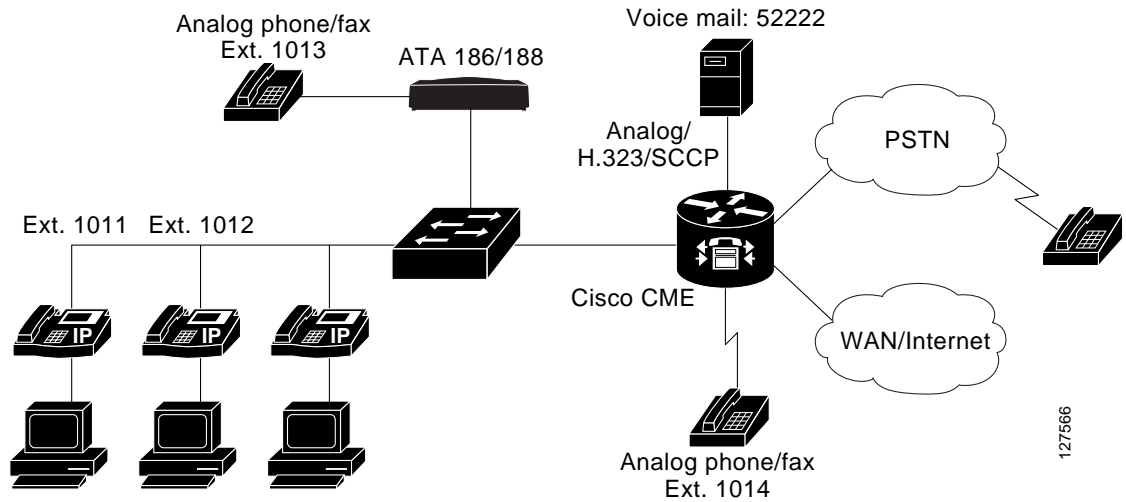
When key-switch mode is selected, IP phones are linked directly to one or more PSTN trunk lines, and this requires manual configuration in addition to using the Cisco CME setup tool. In key-switch mode, each button is associated with one channel; you will need to create two buttons for the same line or extension to support for call waiting, call transfer, and conference. The following features can be used for, but are not limited to, the key-switch mode:

- Shared line appearance
- Paging
- Intercom
- System XML speed dial
- Personal speed dial
- Localization
- Cisco ATA 186/188, Cisco IP Phone 7905G, and Cisco IP Phone 7914 Expansion Model

Standalone Cisco CME—Cisco CME with PSTN Interfaces

In a small branch office with a limit of 120 users where a data router exists with PSTN interfaces, the router can be turned on with Cisco CME features to provide calling capability for the phones locally as shown in [Figure 3](#).

Figure 3 Standalone Cisco CME in a 7905G—Branch Offices



Connection types include the following:

- IP phones through an external switch or external switch (NM-EtherSwitch modules)
- Analog phones/fax through FXS ports
- Analog phones through Cisco ATA-186 or Cisco ATA-188

Call types include the following:

- Local calls
 - IP phone to IP phone
 - IP phone to analog phone among extensions 1011, 1012, and 1013
- Incoming calls from the PSTN to extension 1011, 1012, 1013 by using the following:
 - Connection Private Line Auto Ringdown (PLAR) through FXO
 - DID/Translation Rules through the ISDN
- Outgoing calls through the PSTN
- Incoming and outgoing calls from the WAN/Internet through H.323



Note

- Analog phones can appear as SCCP endpoints through the Cisco ATA-186 or Cisco ATA-188.
- Voice mail can be hosted by the SMB or branch office (see the [“Voice Mail”](#) section on page 26).

The two options for fax support are the following:

- Connect the fax machine to the Cisco ATA that is connected to the Cisco CME: only fax pass-through is supported because the Cisco ATA supports only fax pass-through.
- Connect the fax machine to the FXS port of the Cisco CME router: this supports fax pass-through, T.38, and Cisco fax relay.

Dial-Plan Management

This section includes information about the following topics:

- [Dial-Plan Pattern Enhancement, page 16](#)
- [Cisco CME Registration with the Gatekeeper, page 16](#)

Dial-Plan Pattern Enhancement

The Cisco CME router allows calls to be dialed with an extension number for both internal and external calls. While local IP-phone-to-IP-phone calls can use the extension number to dial directly, Cisco CME allows external calls to be made by extension numbers by appending or stripping of the prefix as configured in the **dialplan-pattern** command.

The **dialplan-pattern** command is used to create a global prefix that can be used to expand the abbreviated extension numbers into fully qualified E.164 numbers. You can configure **dialplan-pattern 1** for extension numbers 5001 to 5099 with the telephone prefix starting with 408555. In the following example, the router sees that 4085555044 matches **dialplan-pattern 1** and uses the **extension-length** keyword to extract the last four digits of the number (5044), and presents this number as the caller ID for the incoming call.

For the following configuration example, when the PSTN connects a Direct Inward Dialing (DID) call for “4085551234” to the Cisco CME system, it also forwards the extension digits “1234” to allow the Cisco CME system to route the call.

```
Router(config)# telephony-service
Router(config-telephony-service)# dialplan-pattern 1 4085551.. extension-length 4 no-reg
```

You can also use the following command to allow the extension numbers with leading zeros to be converted to nonzero leading digits from 400 to 499:

```
Router(config-telephony-service)# dialplan-pattern 1 40855500.. extension-length 3
extension-pattern 4..
```



Note

Cisco CME will create another two POTS dial peers if the **dialplan-pattern** command is set and matches against the ephone-dn number, one for the local extension and one for the complete E.164 direct-dial telephone number that matches a dial-plan pattern: 1234 and 4085551234, respectively. A dial peer will also be created if a secondary number matches a dial-plan pattern.

Cisco CME Registration with the Gatekeeper

In an H.323 network, a gatekeeper can be used to register with the Cisco CME router and IP phones. IP phones can select to register or not to register with the gatekeeper. If IP phones are to register with the gatekeeper, the extension numbers need to be registered as the E.164 numbers. This can be done by assigning the E.164 numbers as the secondary numbers for the ephone-dn and not registering to the primary extension number.


```
Ephone-dn 1
 number 0100 secondary 4085550100 no-reg primary
```

**Note**

The Cisco CME router supports gatekeeper-transparent mode, but does not support gatekeeper-routed-signal mode. See the Cisco IOS gatekeeper documents for details on gatekeeper-transparent mode and routed-signal mode.

Call Transfer and Call Forward

Call transfer and call forward are supported in phases. Cisco CME 2.0 supports only blind transfer using a Cisco CME proprietary mechanism (H.323 nonstandard IE). Cisco CME 2.1 provides call transfer with consultation (also known as supervised or attended transfer) for H.323 calls with H.450.2 standard support using a special TCL script configured on all dial peers. This TCL script is supported with TCL IVR 2.0 in Cisco IOS Release 12.2(11)YT or later. Cisco IOS Release 12.3T also supports hookflash transfer on the analog FXS phones.

H.450.2 is an ITU standard call-transfer supplementary service for H.323 VoIP. However, current third-party H.323 products do not support H.450.x because peer-to-peer call transfers are not generally implemented.

This section contains information about the following:

- [H.450.2 Call Transfer, page 17](#)
- [H.450.2 Call Transfer Configuration, page 18](#)
- [H.450.3 Call Forward, page 19](#)
- [Call Transfer/Forward Scenarios, page 19](#)
- [H.450.2 and H.450.3 Deployment Issues, page 22](#)

H.450.2 Call Transfer

The H.450.2 call flow is as follows:

- A calls B; B transfers to C with a consultation call to C.
- B talks with C; B commits a transfer; B requests and receives an H.450.2 consultation ID from C.
- B sends transfer request to A with consultation ID.
- A calls C with consultation ID in the call setup message.
- A to C call succeeds; A and C disconnect the call to B.

The consultation ID is a central component of the H.450.2 mechanism that helps route the transferred call to the right physical line by ensuring that the A-to-C call goes to the correct destination, and it resolves issues where multiple phone lines have the same telephone number.

The advantages of the H.450.2 call flow include the following:

- Final A-to-C call path is optimal with no “hairpin” media or control path.
- Call parameters for A-B, B-C, and A-C can all be different (for example, different codecs).
- H.450.2 is very scalable. Once transfer is committed, all resources at B are released.
- There is no H.450.2 limit to the number of times a call can be transferred.

The disadvantages of the H.450.2 call flow include the following:

- All H.323 and VoIP routers in the network need to support H.450.2.
- Call transfer may drop or be incomplete if participating endpoints do not support H.450.2.
- H.450.2 will not run on “legacy” Cisco 2610, Cisco 2620, and Cisco 3620 routers because of a lack of H.450 support.
- H.450.2 requires Cisco IOS Release 12.2(11)YT or Cisco IOS Release 12.2(15)T with Cisco CME 2.1 with the H.450 call transfer script.
- H.450.2 requires Cisco IOS Release 12.2(15)ZJ and Cisco CME 3.0 features with built-in H.450 support.
- H.450.12 supplementary services capabilities exchange between routers is not implemented in Cisco IOS Release 12.2.(15)ZJ3.
- Automatic detection of H.450.2 (or H.450.3) endpoint capability is not supported.

H.450.2 billing issues include the following:

- Because the final call is originated as “A calls C,” it is unknown who pays for the A-to-C call.
- An enhanced billing system is needed to identify that since B requested the transfer, B should pay for A-to-C call (or at least a portion of the cost). However, this is not an issue in enterprise networks, where the A device may actually be just a PSTN ingress gateway, and B and C are both internal phones.

H.450.2 Call Transfer Configuration



Note

With Cisco CME 3.0 software starting from Cisco IOS Release 12.2(15)ZJ, “application bator” is not needed for IP phones and incoming dial-peer configuration. See the [Cisco IOS Telephony Services Version 2.1](#) document for Cisco CME (ITS) 2.1 specifics.

```
dial-peer voice 100 pots
 destination-pattern 9.T
 port 1/0/0

dial-peer voice 4000 voip
 destination-pattern 4...
 session-target ipv4:1.1.1.1

telephony-service
 transfer-pattern 4...
 transfer-system full-consult
```

All transfers on an individual Cisco CME router use either H.450.2 or the Cisco CME proprietary mechanism.

The **transfer-system** command syntax is the following:

transfer-system blind {local-consult | full-consult | full-blind}

- **blind**—Default, backwards compatible to Cisco CME 2.0.
- **local-consult**—Intended primarily for VoFR, blind transfer only for VoFR in Cisco IOS Release 12.2(8)T.
- **full-consult**—Uses H.450.2 for transfer with consult.
- **full-blind**—Uses H.450.2 and default transfers to blind transfers.

Local Consult

For a transfer from one local IP phone to another local IP phone, local consult emulates a transfer with consult by allowing the transferor to independently call the transfer-to party and then trigger a call-pickup-on-hold (of the transferee) by the transfer-to destination phone. There is no consultation ID mechanism, so the transfer-to number must be unique for local consult to work correctly.

In ephone-dn configuration mode, the **transfer-mode** command allows you to override the system default **transfer-system** command setting (**full-consult** or **full-blind**) for an individual ephone-dn or line.

Restrictions and Limitations

- You cannot change the call transfer system from H.450.2 to the Cisco CME proprietary mechanism.
- FXS analog (hookflash) transfer functionality does not support call transfer or call forwarding for more than one consultation call, such as A calls B, and B places consultation call to C but is transferred or forwarded to D. The limitation is that D cannot call transfer or call forward B's call to another party. This restriction does not apply to IP phones.

H.450.3 Call Forward

H.450.3 call forward is an ITU standards based alternative to Cisco CME proprietary H.323 nonstandard IE forwarding for busy, no-answer, and call-forward all. H.450.3 does not require the H.450 call transfer script in Cisco CME 3.0.

Cisco CME proprietary forwarding attempts to resolve forwarding for the local forward-to destination within the router first; for example, local call hunting. However, H.450.3 always returns the call to the originator gateway, even if the forwarder and forward-to numbers are on the same Cisco CME. H.450.3 is an optimal method for forwarding to PSTN numbers, where the destination PSTN number, best accessed locally, is the call originator; for example, forward to 1-800.

```
telephony-services
forward-pattern 4...
```

If forward pattern is specified or configured, calls from the pattern, such as 4001 (the calling number, not the called number), will be forwarded using H.450.3, while all other calling parties will be forwarded using Cisco CME proprietary forwarding for backwards compatibility unless "forward-pattern.T" is configured to forward all calls using H.450.3.

Call Transfer/Forward Scenarios

[Figure 4](#), [Figure 5](#), [Figure 6](#), [Figure 7](#), and [Figure 8](#) show the five typical scenarios for PSTN, H.323, and VoIP calls to transfer/forward the calls from one system to another.

[Figure 4](#) shows extension 1001 calling 6001 and being transferred to 6001. There is no H.323 or H.450.

Figure 4 Scenario 1

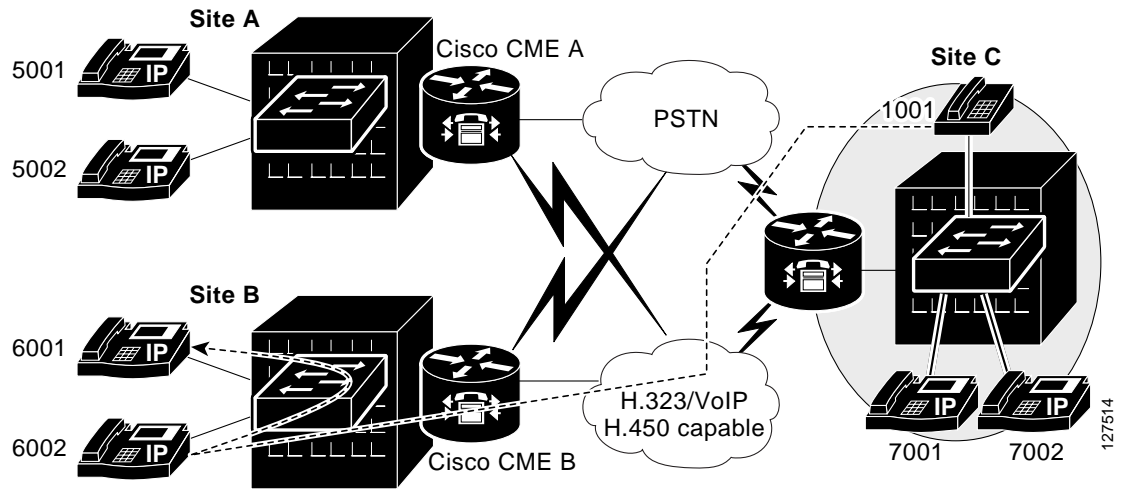


Figure 5 shows a local hairpin transfer. Extension 7001 calls 5002 and is transferred to 5001 using H.450. Extension 7001 calls 5002 and uses the consultation ID sent by extension 5002 to call 5001.

Figure 5 Scenario 2

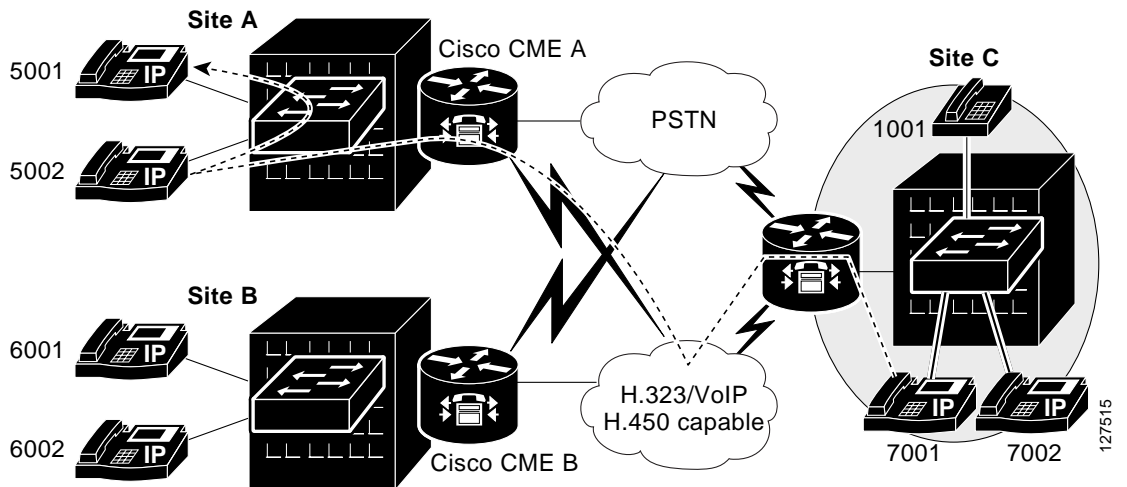


Figure 6 shows an on-net hairpin transfer. Extension 7001 calls 5002 and is transferred to 6002 using H.450. Extension 7001 calls 5002 and uses the consultation ID sent by extension 5002 to call 6002.

Figure 6 Scenario 3

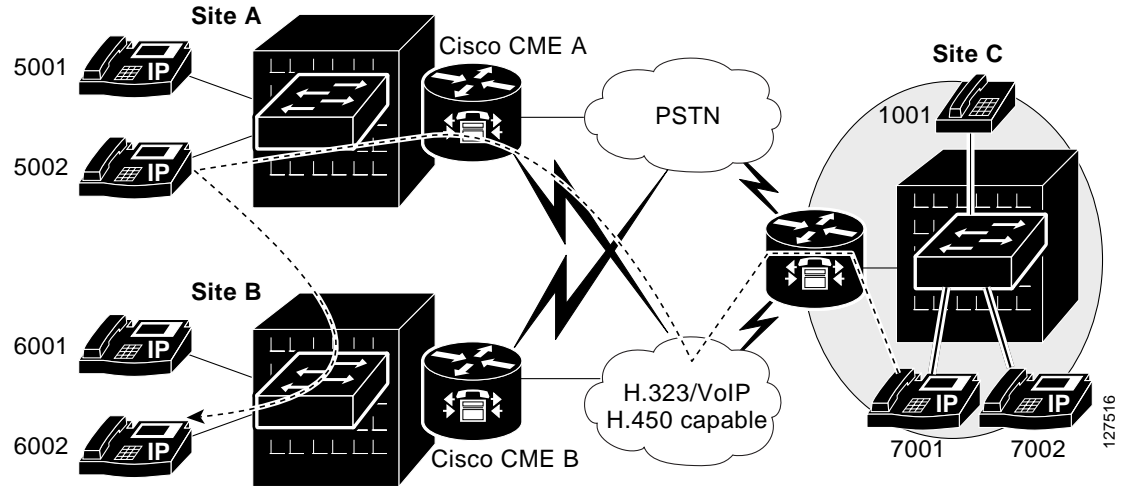


Figure 7 shows on-net and local-hairpin transfer. Extension 7001 calls 5002 and is transferred to 6002, and then to 6001 using H.450. Extension 7001 calls 5002, uses the consultation ID from 5002 to call 6002, and gets a consultation ID for 6001 to call 6001.

Figure 7 Scenario 4

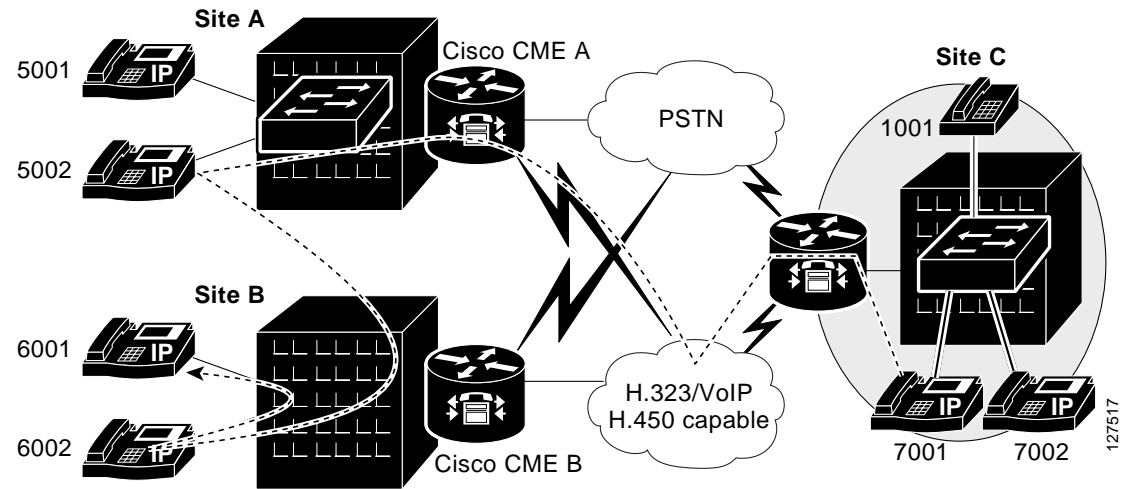
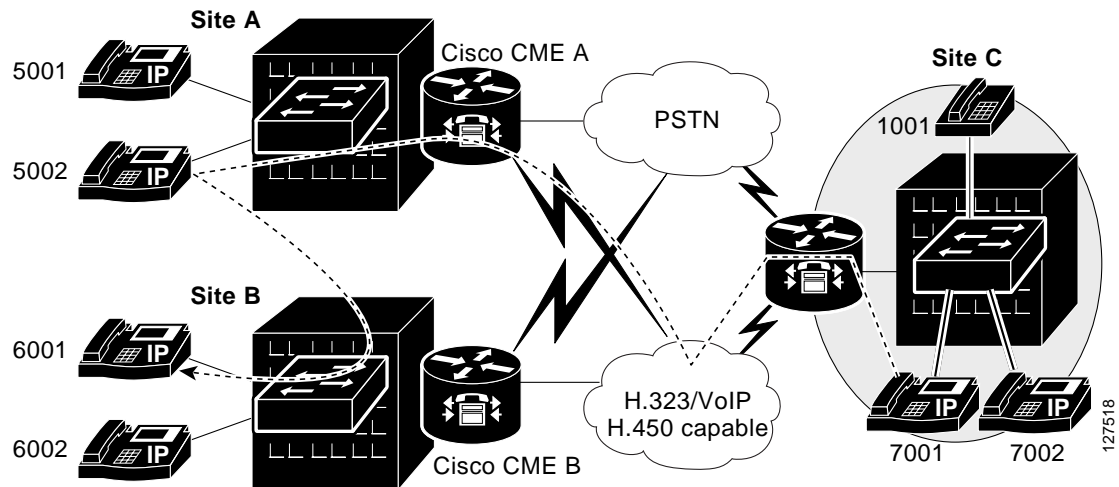


Figure 8 shows on-net call forward. Extension 7001 calls 5002 and is forwarded to 6001 using H.450.

Figure 8 Scenario 5



H.450.2 and H.450.3 Deployment Issues

The following are issues to consider when deploying H.450.2 and H.450.3:

Built-In Support for H.450.2/H.450.3

Cisco CME 3.0 has built-in support for call transfer/forward in H.450.2/H.450.3 for IP phones. The new default session application introduced in Cisco CME 3.0 is an Application Framework Session application that includes support for call transfer requests. Thus, you will not need to download or configure the H.450 call transfer script manually as in Cisco CME 2.1. However, this new default session application does not support analog hookflash transfer using phones connected to the FXS ports of the Cisco CME router. Call transfer/forward for analog phones still requires the H.450 call transfer script.

Though you will not need to configure the H.450 call transfer script for all dial peers as in Cisco CME 2.1, configuration on call transfer types is still needed. The following is a consultative transfer configuration:

```
telephony-service
.
.
.
transfer-system full-consult
transfer-pattern .....
.
.
ephone-dn 1
transfer-mode consult
```

Built-In Support for H.450.2/H.450.3 Versus Existing Auto-Attendant Script

The Auto-Attendant script shipped with Cisco CME 2.0 and 2.1 does not work with Cisco CME 3.0. If the Auto-Attendant script takes a call, the script either cannot hand off the call to the H.450 call transfer script or will hand off the call to the Cisco CME 3.0 code with built-in H.450 support; thus call transfer

or call forward will fail. You can only run the Auto-Attendant feature or H.450 call transfer, but you cannot run both features together. For Auto-Attendant feature support with the Cisco CME 3.0 default session application infrastructure, changes will be needed for the AA script to hand off the call to the H.450 call transfer script and/or the built-in default session application in Cisco IOS software, and changes are also needed for the H.450 call transfer script and the built-in default session application in Cisco IOS software to receive or accept the call using handoff.

H.450 Everywhere in the Network

Call transfer and call forward support in Cisco CME 3.0 requires that all voice routers in the network have appropriate call transfer support for transfer to work correctly. When H.450.2 and H.450.3 are deployed in H.323/VoIP networks, all voice routers need to be upgraded to understand H.450.2/H.450.3 messages. H.450.3 forwarding will allow for staged upgrade, but routers need to be configured to explicitly identify which calling party numbers support H.450.3 and which do not. H.450.2 and H.450.3 can be enabled independently.

In case some voice gateways/routers in the network do *not* understand H.450.2 and H.450.3, the workaround is to use local consult by upgrading all routers to Cisco CME 2.0 software with Cisco IOS Release 12.2(8)T or Cisco IOS Release 12.2(11)T. However, local consult does not work with the Cisco AS5300, Cisco AS5400, or Cisco AS5800 in which only blind transfer is supported.

Another alternative for call transfer/forward on H.323/VoIP endpoints of non-Cisco CME routers or third-party gateways is to use a pair of loopback-dns on the Cisco CME router to terminate and regenerate a call locally.

Loopback-dn Support for Call Transfer and Call Forwarding on Cisco and Third-Party Gateways

Before starting on this session, think hard and make up your mind if you do need to use loopback-dns and be aware that it is nontrivial to configure loopback-dns and that loopback-dns have many issues. It is recommended that you upgrade all the routers for H.450 transfer support. If you cannot have H.450 across the network, upgrade all routers with Cisco IOS Release 12.2(8)T or Cisco IOS Release 12.2(11)T to use local consult; if you cannot and still really need the call transfer support, the alternative of using loopback-dn is a last choice for the following reasons:

- Loopback-dn support is not standard-based H.450.
- There is no DSP or transcoding.
- All call segments must be using the same voice codec, and other call parameters, such as DTMF relay, must be the same.
- Only G.711 is supported. For example, when A and B are connected to the Cisco CME router, A calls B (G.711 is used), B transfers to C across the WAN, and the call will keep the same codec, G.711. This could be a problem because calls in G.711 require more WAN bandwidth, and voice quality will be an issue.
- Control of caller-ID display is difficult.
- Will not pass VoIP T.38 fax-relay calls.
- Uses up ephone-dns and consumes more memory space.

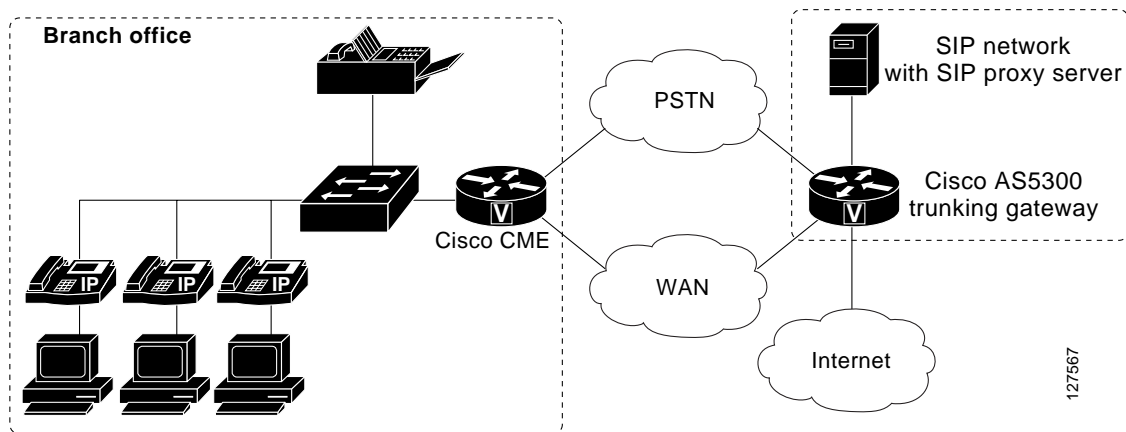
When IP phones are connected to the same standalone Cisco CME router, call transfer call forward does not need any loopback-dn support because there is no VoIP or incompatible endpoints involved. However, the five scenarios shown in [Figure 4](#), [Figure 5](#), [Figure 6](#), [Figure 7](#), and [Figure 8](#) in the “[H.450.3 Call Forward](#)” section on page 19 will require loopback-dn support if Site A, B, and/or C do not use all Cisco CME routers or support H.450.

Cisco CME in SIP Networks

When a Cisco CME router is deployed in SIP networks, Cisco CME integration with SIP is via SIP gateway trunks to support basic calls. SIP Redirect and SIP Refer can be used for call transfers and call forwarding. Consultative transfer should work. Because IP phones do not support in-band DTMF (RFC 2833) in SIP networks (note that Cisco CME integration with H.323 networks uses DTMF relay: H.245-alphanumeric), Cisco CME 3.0 has added Cisco proprietary Notify-based Out-of-band DTMF relay for IP phones in SIP networks. Cisco CME integration with SIP networks uses unsolicited Notify for DTMF relay. Unsolicited Notify is Cisco proprietary and is symmetrical DTMF relay that has to be negotiated during the call setup.

Figure 9 shows how Cisco CME can be deployed in a SIP network.

Figure 9 Deploying Cisco CME in SIP Networks



Note

SIP phones are not supported with Cisco CME, only with SIP-SRST.

The following SIP gateway enhancement features are added:

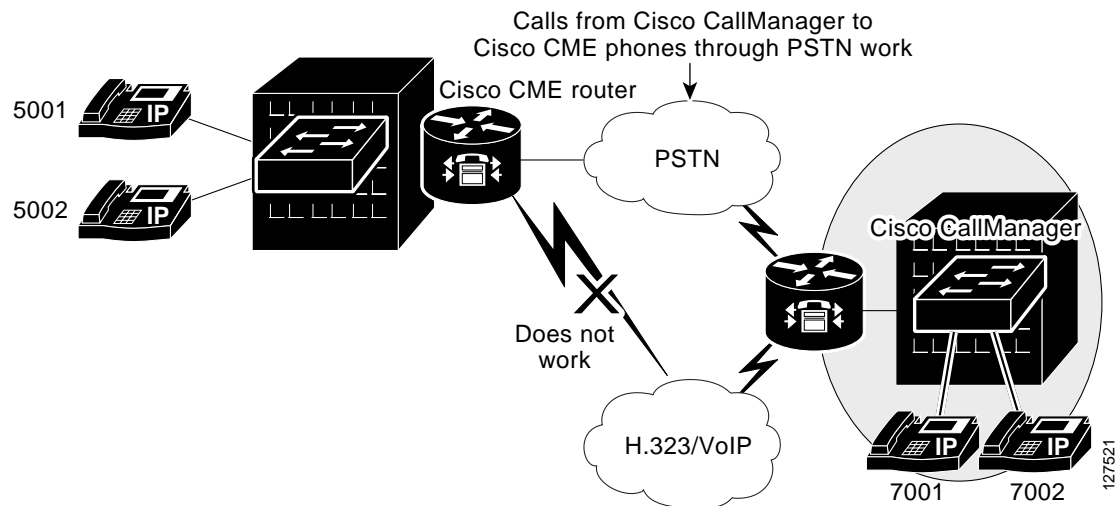
- SIP Register
 - Register E164 numbers for Cisco CME ephone-dns and analog FXS ports to SIP Registrar/Proxy.
 - Enhanced command-line interface (CLI) under dial-peer (register e164) to support both SIP and H.323.
- Out-of-Band DTMF Relay
 - Support for unsolicited NOTIFY based out-of-band DTMF.
 - Bidirectional DTMF relay, negotiated during call setup.
 - Needed because SCCP IP phones cannot do in-band digit relay or RFC 2833.
 - Cisco proprietary and works with Cisco Unity and PGW Call Agent.
- Unsolicited Notify for MWI
 - For voice mail that does not support full subscribe/notify for MWI (SIP Cisco Unity server).
 - SIP Cisco Unity server only supports unsolicited NOTIFY for MWI.

- Voice mail sends unsolicited Notify to SIP Proxy that delivers to the appropriate MWI target phone.
- Cisco CME accepts SIP unsolicited NOTIFY from the voice-mail system and then converts the MWI message to SCCP message to turn MWI lamp on SCCP phone to on/off.

Cisco CME Integration with Cisco CallManager

Cisco CallManager uses Empty Capability Set (ECS), a nonstandard protocol, which does not easily support multiple transfers of same call but adds signaling delay for each transfer. Cisco CME does support incoming ECS requests from other voice gateways, but Cisco CME will not initiate an ECS transfer request. [Figure 10](#) illustrates when a Cisco CME router is integrated with Cisco CallManager through PSTN and H.323.

Figure 10 Cisco CME Router Integrated with Cisco CallManager Through PSTN and H.323



Cisco CME integration with Cisco CallManager through PSTN does work; however, Cisco CME integration with Cisco CallManager through H.323 has some interoperability issues, such as lack of ring-back tones, dropping of calls when transferred calls are initiated from the Cisco CME site, one-way voice path, and lack of supplementary services. The workaround for Cisco CME integration with Cisco CallManager through H.323 is to use the loopback-dns. However, loopback-dn is quite complex because configuration for loopback-dns is nontrivial and there are many issues to be aware of. Please set your expectations appropriately.



Note

Cisco CallManager will add a SIP interface, so interoperability between the two will likely be SIP based in the future.

Cisco CME Migration to Cisco CallManager and Cisco SRST

The Cisco CME deployment solution is designed to fully protect your investment if you decide to migrate to a Cisco CallManager and Cisco SRST solution because of some specific feature needs and/or they outgrow the 120-user limit. The full-featured data router providing Cisco CME functionality can be

transitioned into a high-availability gateway in a centralized Cisco CallManager and Cisco SRST design with only some configuration changes. The Cisco CME feature license and phone seat licenses (also called user licenses) can be converted to Cisco CallManager and Cisco SRST licenses. There will be no additional upgrade issues that customers will have to deal with.

Voice Mail

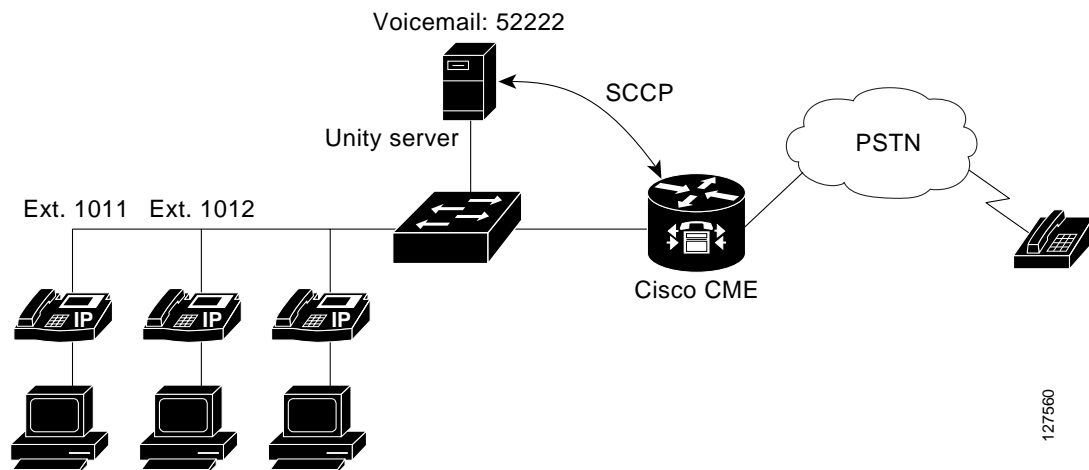
Cisco CME can be integrated with voice-mail systems using SCCP, analog DTMF, H.323, and SIP protocols. This section contains information about the following:

- [SCCP Integration with Cisco Unity Server, page 26](#)
- [Analog DTMF Integration with Active Voice Reception and Octel Voice-Mail System, page 30](#)
- [H.323 Integration with SAS and SSAM, page 35](#)
- [SIP Integration with Cisco Unity Express, page 38](#)
- [Voice-Mail Integration in a Centralized Environment, page 38](#)

SCCP Integration with Cisco Unity Server

[Figure 11](#) shows the architecture of how Cisco CME and Cisco Unity are connected in the network for voice-mail integration.

Figure 11 Cisco CME Voice-Mail Integration with Cisco Unity Server



The Cisco CME router registers Cisco Unity ports (vm-device-id CiscoUM-VI2) as SCCP devices/ephones where the voice-mail pilot number is configured as an ephone-dn, and the vm-device as an ephone. For a four-port Cisco Unity server integration, you must configure four ephone-dns and four ephones for the four voice-mail ports and four voice-mail device IDs accordingly. Cisco CME voice-mail integration with Cisco Unity supports the following:

- Direct access to the voice-mail system. To access your mailbox from an IP phone, you may press the “messages” button on the phone or dial the voice-mail number, such as 50100. You will be asked to enter your PIN number to listen to your messages. To access your mailbox from PSTN, you may dial the voice-mail number, such as 4085550100, and then enter your extension and PIN number. Once you are authenticated, you can listen, cancel, and store your messages.
- Call forward all/busy/noan (no answer) to personal greeting. When a calling party places a call to an extension 1011 connected to the Cisco CME router, and the extension is configured with the call forward option, the call will be forwarded to Cisco Unity voice mail for extension 1011 when call no answer/all/busy. Cisco CME communicates with the Cisco Unity server through the SCCP protocol. When the call is forwarded to the Cisco Unity voice-mail server, the calling number, called party number, and redirect number are all forwarded to the Cisco Unity server with ANI/DNIS/RDNIS support; thus the call is forwarded to the called extension’s own voice-mail box and the personal greeting can be heard.
- MWI. Upon receiving the MWI status from the Cisco Unity voice-mail system for an extension, the Cisco CME router can signal the IP phone to turn the MWI lamp on/off.
- MWI Relay. The MWI relay method applies to a centralized environment in which a single voice-mail system is shared among multiple Cisco CME routers in remote branch offices.

Configuration

Configuration includes the following tasks:

- [Configure the “Messages” Button to Access the Voice-Mail System \(Pilot Number\) Directly, page 27](#)
- [Configure and Bind the Voice-Mail Ports, page 27](#)

Configure the “Messages” Button to Access the Voice-Mail System (Pilot Number) Directly

You may configure “voicemail 52222” in telephony-service configuration mode:

```
telephony-service
 voicemail 52222
```

Pressing the messages button on the IP phone or dialing 52222 will let you access the Cisco Unity voice-mail system.

Configure and Bind the Voice-Mail Ports

Configuring and binding the voice-mail ports consists of the following tasks:

- Configuring and defining the voice-mail number (4 ports are used). To integrate with a four-port Cisco Unity server, configure four ephone-dns for the four ports on the Cisco Unity server with the same voice-mail number 52222 for answering calls and MWI with preference 0, 1, 2, and 3 so if the first port is busy, it will go to the second port and so on. Or you can configure three ephone-dns for the three ports on the Cisco Unity server with the same voice-mail number 52222 for answering calls and the fourth one with number 52223 equivalent to the fourth port on Cisco Unity primarily for dial-out MWI.

```
ephone-dn 32
 number 52222
 name "VOICEMAIL1"
 preference 0

ephone-dn 33
 number 52222
```

```

name "VOICEMAIL2"
preference 1

ephone-dn 34
number 52222
name "VOICEMAIL3"
preference 2

ephone-dn 35
number 52222
name "VOICEMAIL4"
preference 3

! Or configure a dedicated port for MWI only.
! ephone-dn 35
! number 52223
! name "MWI ONLY"

```

- Bind the voice-mail device ID to the voice-mail port number.

```

ephone 5
vm-device-id CiscoUM-VI1
button 1:32

ephone 6
vm-device-id CiscoUM-VI2
button 1:33

ephone 7
vm-device-id CiscoUM-VI3
button 1:34

ephone 8
vm-device-id CiscoUM-VI4
button 1:35

```

- Configure call forwarding to voice mail. You may configure call forward all/busy/noan to the voice mail as follows:

```

ephone-dn 1
number 1011
call-forward busy 52222
call-forward noan 52222 timeout 10

! or
! call-forward all 52222

ephone-dn 2
number 1012
call-forward busy 52222
call-forward noan 52222 timeout 10
! or
! call-forward all 52222

```

- Configure the MWI. The Cisco Unity voice-mail system is able to communicate MWI status with the Cisco CME router so that the Cisco CME router can signal the IP phones to turn the MWI lamp on and off. Use an ephone-dn number to define one number for MWI on and one number for MWI off. These numbers must match those used during Telephone Application Programming Interface (TAPI) service provider (TSP) installation. The MWI target DN will be taken from the calling party number. This is the mechanism normally used for SCCP-based MWI.



Note To ensure that MWI works, the Cisco Unity server and MWI status must be restarted and resynced every time a Cisco CME router is rebooted and reloaded.

```
ephone-dn 30
  number 8000
  mwi on
```

```
ephone-dn 31
  number 8001
  mwi off
```

Calls to 8000 will turn the MWI on, and calls to 8001 will turn the MWI off for the extension indicated by the calling-party information supplied through caller ID.

Configuration Example



- Note**
- Cisco CME uses the same Cisco Unity SCCP TSP (AvCisco TSP) supported by Cisco CallManager. Cisco CME registers Cisco Unity ports as SCCP devices and ephones.
 - The voice-mail device ID must match the voice-mail port number on Cisco Unity SCCP TSP (AvCisco TSP).
 - The CiscoUM-VI# is the default voice-mail device ID in AvCisco TSP installation.

```
.
.
.
telephony-service
  voicemail 52222

ephone-dn 30
  number 8000
  mwi on

ephone-dn 31
  number 8001
  mwi off

ephone-dn 32
  number 52222
  name "VOICEMAIL1"
  preference 0

ephone-dn 33
  number 52222
  name "VOICEMAIL2"
  preference 1

ephone-dn 34
  number 52222
  name "VOICEMAIL3"
  preference 2

ephone-dn 35
  number 52222
```

```
name "VOICEMAIL4"  
preference 3  
  
! or  
! ephone-dn 35  
! number 52223  
! name "MWI ONLY"  
.  
.  
.  
ephone 5  
vm-device-id CiscoUM-VI1  
button 1:32  
  
ephone 6  
vm-device-id CiscoUM-VI2  
button 1:33  
  
ephone 7  
vm-device-id CiscoUM-VI3  
button 1:34  
  
ephone 8  
vm-device-id CiscoUM-VI4  
button 1:35
```

Analog DTMF Integration with Active Voice Reception and Octel Voice-Mail System

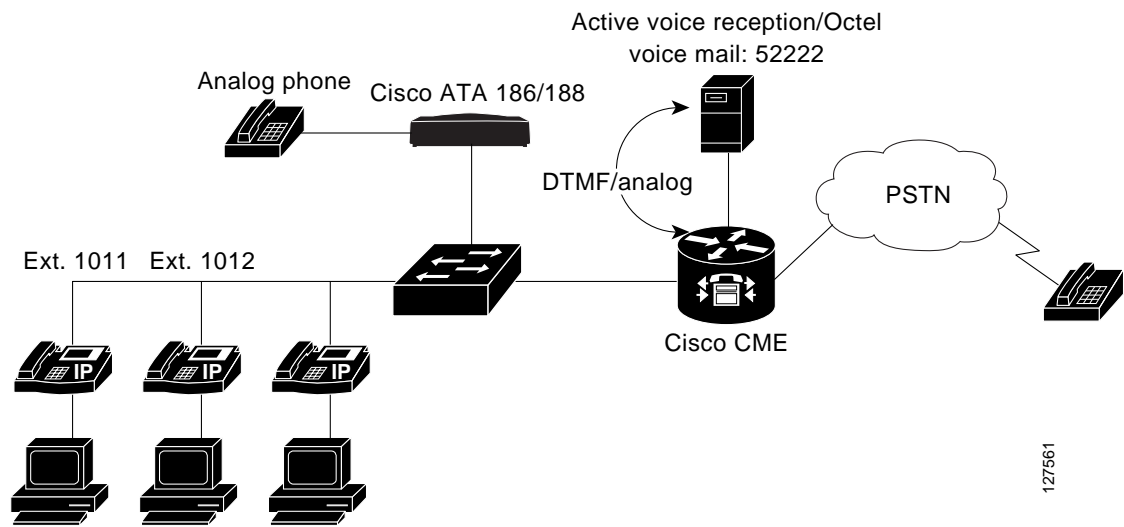
This section contains information about the following:

- [Analog DTMF Integration with Active Voice Reception, page 30](#)
- [In-Band DTMF Integration with Octel, page 33](#)

Analog DTMF Integration with Active Voice Reception

[Figure 12](#) shows that the connection between Cisco CME and active voice reception/Octel voice-mail system is through FXS using analog DTMF.

Figure 12 Cisco CME Voice-Mail Integration Through Analog DTMF



The voice-mail system is connected to the FXS port of the router and is treated as a normal extension for the Cisco CME router. For DTMF integrations, information on how to route incoming or forwarded calls in the form of DTMF digits is sent by the Cisco CME router, and message waiting lamp codes are sent from the voice-mail system in the form of DTMF packets. Voice-mail systems are designed to respond to DTMF after the system has answered the incoming calls.

DTMF integrations support the following features:

- Direct access to the voice-mail system by pressing the “message” button. You can access your voice mail from an IP phone by pressing the button on the phone. When the voice-mail system answers the call, the Cisco CME router sends a DTMF packet to inform the voice-mail system that this is a direct call from extension 1011. You will be automatically put into your own voice mailbox and prompted to enter the option for checking messages.
- Call forward busy/noan/all to personal greeting. When extension 1011 calls extension 1012, 1012 is busy or no answer, extension 1011 will be forwarded to 1012’s voice mail and 1012’s personal greeting will be heard. To route calls to the extension’s voice mail, the voice-mail system must receive instructions on where to route the call. Note that different personal greetings can be heard when different values are set to the DTMF patterns for call forward busy and call forward no answer. Please refer to the configuration section for details.

Call forward scenario includes the following two scenarios:

- Call forward calls coming from FXO to local extension
 - Call forward calls coming from FXO to voice-mail system through VoIP
- MWI. If extension 1011 has messages, the voice-mail system will send an MWI status to notify the Cisco CME router that extension 1011 has messages, and the Cisco CME router will then signal the phone to light the lamp. In order to light message waiting lamps, the Cisco CME router must receive information on what lamp to light from the voice-mail system.

The DTMF integration configuration on the Cisco CME router works with any analog voice-mail system. Configuration includes the following tasks:

- [Configure the “Messages” Button to Access the Voice-Mail System \(Pilot Number\) Directly, page 32](#)
- [Configure Call Forwarding to the Voice-Mail System, page 32](#)
- [Configure Message Waiting Indication \(MWI\), page 33](#)

Configure the “Messages” Button to Access the Voice-Mail System (Pilot Number) Directly

You may configure “voicemail 33333” in telephony-service configuration mode as shown in the following example:

```
telephony-service
  voicemail 33333
```

Pressing the messages button on the IP phone or dialing 33333 will let you access the voice-mail system.

Configure Call Forwarding to the Voice-Mail System

The Cisco CME router communicates with the analog voice-mail system by sending DTMF patterns. The following voice-mail integration configuration includes four call forward scenarios when call forward to the voice-mail system is configured with DTMF patterns set to 4, 5, 6, and 7, respectively. This also requires that the active voice reception system be accordingly configured with correct patterns.

pattern ext-to-ext no-answer

The Cisco CME router sends 5 to notify the voice-mail system to play personal greetings for no answer when a call coming from one extension to another is forwarded with an answer.

pattern ext-to-ext busy

The Cisco CME router sends 7 to notify the voice-mail system to play personal greetings for busy when a call coming from one extension to another is forwarded with busy.

pattern trunk-to-ext no-answer

The Cisco CME router sends 4 to notify the voice-mail system to play personal greetings for no answer when a call coming from FXO to an extension is forwarded with no answer.

pattern trunk-to-ext busy

The Cisco CME router sends 6 to notify the voice-mail system to play personal greetings for busy when a call coming from FXO to an extension is forwarded with busy.

```
.
.
.
telephony-service
  load 7960-7940 P00303020209
  max-ephones 48
  max-dn 100
  ip source-address 10.10.10.199 port 2000
  create cnf-files
  application bator
  max-conferences 6
  transfer-pattern .T
  voicemail 33333
  transfer-system full-consult
```



```

vm-integration
pattern direct 2 CGN *
pattern ext-to-ext no-answer 5 FDN * CGN *
pattern ext-to-ext busy 7 FDN * CGN *
pattern trunk-to-ext no-answer 4 FDN * CGN *
pattern trunk-to-ext busy 6 FDN * CGN *

ephone-dn 2
number 30002
description CME-VM-Dept
name User#30002
call-forward busy 33333
call-forward noan 33333 timeout 10
application bator
translate called 2

ephone-dn 4
number 30001
description CME-VM-Dept
name User#30001
call-forward busy 33333
call-forward noan 33333 timeout 10
application bator
translate called 2

ephone-dn 14
number 31002
name User#ATA-3
call-forward busy 33333
call-forward noan 33333 timeout 10
application bator

ephone-dn 15
number 31003
name User#ATA-4
call-forward busy 33333
call-forward noan 33333 timeout 10
application bator

```

Configure Message Waiting Indication (MWI)

The following is an example MWI configuration:

```

ephone-dn 25
number A1.....*
mwi on

ephone-dn 26
number A2.....*
mwi off

```

In-Band DTMF Integration with Octel

Configuration for Octel integration is very similar to the active voice reception integration. The Cisco CME configuration recommendations specific to Octel systems are listed below:

- Octel does not distinguish between ext-to-ext and trunk-to-ext transfers, so DTMF patterns for ext-to-ext and trunk-to-ext should be configured with the same values on the Cisco CME router. For example, in the validation example the ext-to-ext no-answer pattern is **5 CGN * FDN** so the trunk-to-ext no-answer pattern should also be **5 CGN * FDN**.

- The MWI ephone-dn should not use the **T** wildcard, but should use the wildcard character (.) to specify the exact extension length. Also, an asterisk (*) should be used before and after the called party ID. For example, if Cisco CME phones use four-digit extensions and the MWI ON prefix is 3000 and the MWI OFF prefix is 3001, the ephone-dn for MWI ON will be **3000*....*** and the ephone-dn for MWI OFF will be **3001*....***.
- The topology that has been validated is as follows: the analog card on an Octel system is connected to FXS ports on the Cisco CME router, with at least one FXS port dedicated to MWI. Octel integration was validated using a Cisco 2651XM router with one NM-2V and one VIC-2FXS installed.
- The test cases that have been validated for Octel integration are as follows:
 - Direct access to voice mail using “Messages” button on Cisco CME phone
 - Call forward all/busy/no-answer incoming call from local Cisco CME phone to voice mail
 - Call forward all/busy/no-answer incoming call from local analog phone to voice mail
 - Call forward all/busy/no-answer incoming call from FXO port to voice mail
 - Call forward all/busy/no-answer incoming VoIP call to voice mail
 - MWI on/off for all cases listed above

The following is a sample of Cisco CME DTMF integration settings. Voice port 1/0/0 is dedicated to voice traffic. All settings relevant to DTMF integration have been highlighted.

```

.
.
.
dial-peer voice 5000 pots
  application bator
  destination-pattern 5000.....
  port 1/0/0

telephony-service
load 7960-7940 P00303020209
max-ephones 48
max-dn 192
ip source-address 10.4.28.5 port 2000
create cnf-files
application bator
transfer-pattern 2...
transfer-pattern 5...
voicemail 5000
transfer-system full-consult

vm-integration
pattern direct 2 CGN
pattern ext-to-ext no-answer 5 CGN * FDN
pattern ext-to-ext busy 7 CGN * FDN
pattern trunk-to-ext no-answer 5 CGN * FDN
pattern trunk-to-ext busy 7 CGN * FDN

ephone-dn 1
number 1000
description octeltest
name test1
call-forward noan 5000 timeout 5
application bator
no huntstop
.
.
.

```

```

ephone-dn 4
 number 1001
 name test2
 preference 1
 call-forward busy 5000
 call-forward noan 5000 timeout 5
 application bator

ephone-dn 100
 number 3000*....*
 mwi on
ephone-dn 101
 number 3001*....*
 mwi off

ephone 1
 mac-address 0030.94C2.9852
 button 1:1 2:2

ephone 2
 mac-address 00D0.59E1.F0C8
 button 1:3 2:4
.
.
.

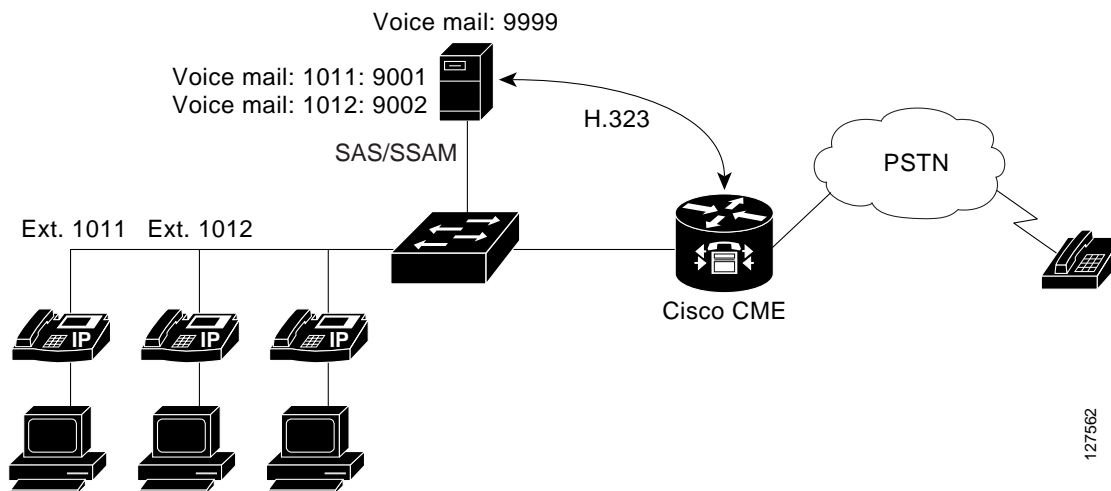
```

H.323 Integration with SAS and SSAM

H.323 can be integrated with Stonevoice Application Suite (SAS) and Soft Switch Answering Machine (SSAM). SAS is a common web-based environment running on Windows that allows management of service system parameters and user database shared by all available Stonevoice applications for Cisco CME. SSAM is a unified messaging solution built to integrate and extend the functionality of Cisco CME. SSAM version 2.0 for Cisco CME is fully integrated with SAS.

Figure 13 shows the architecture of how Cisco CME and SAS/SSAM are connected in the network.

Figure 13 Cisco CME Voice-Mail Integration with SAS and SSAM via H.323



127562

The Cisco CME router can be integrated with SAS/SSAM software-based voice-messaging system to provide a voice-mail solution. Each directory number (extension) configured on Cisco CME must also have an associated voice-mail number to forward the calls based on the “call-forward ephone-dn” statement within Cisco CME. All voice-mail numbers are managed by the SAS/SSAM system. Communication between the Cisco CME router and the SAS/SSAM system is via H.323.

Cisco CME voice-mail integration with SAS/SSAM supports the following:

- Direct access to the voice-mail system. To access your mailbox from an IP phone, you may press the “messages” button on the phone or dial the voice-mail number (for example, 9999), and then you will be asked to enter your PIN to listen to your messages. To access your mailbox from PSTN, you may dial the voice-mail number (for example, 9999), and then enter your extension and PIN. Once you are authenticated, you can listen, cancel, and store your messages.
- Call forward all/busy/noan (no answer) to personal greeting. When a calling party places a call to an extension 1011 (or 1012) connected to the Cisco CME router, and the extension is configured with the call forward option, the call will be forwarded to extension 1011 (or 1012)’s voice mail on SSAM when 1011 (or 1012) is busy and/or no answer after the configured no answer time expires. Cisco CME communicates with the SSAM system via H.323. Cisco CME must have a VoIP dial peer to route the calls to the SSAM system. Extension 1011 (or 1012) must have a unique voice-mail number (for example, 9001 or 9002) created on the SSAM system so that the caller can be put into extension 1011 (or 1012)’s voice-mail number 9001 (or 9002) when 1011 (or 1012) is busy or not answered because the called number 1011 (or 1012) is not passed with the voice-mail number in the H.323 messages.
- Message waiting indication (MWI). Upon receiving the MWI status from the SAS/SSAM voice-mail system for an extension, the Cisco CME router can signal the IP phone to turn the MWI lamp on/off.

Configuration

Configuration on Cisco CME includes the following tasks:

- [Configure a VoIP Dial Peer to Access the Voice-Mail System, page 36](#)
- [Configure the “Messages” Button to Access the Voice Mail Directly, page 37](#)
- [Configure Call Forwarding to Voice Mail, page 37](#)
- [Configure MWI, page 37](#)



Note

SAS/SSAM application must be restarted when changes are made to the Cisco CME router.

Configure a VoIP Dial Peer to Access the Voice-Mail System

To enable access to the voice-mail system, configure a VoIP dial peer with a destination pattern matching the voice-mail extension and route the calls to the voice-mail system. The following shows that all calls to a number 9... will be routed to 172.19.153.120, the SSAM service.

```
dial-peer voice 100 voip
destination-pattern 9...
session target ipv4:172.19.153.120
dtmf-relay h245-alphanumeric
codec g711ulaw
```

Configure the “Messages” Button to Access the Voice Mail Directly

```
telephony-service
 voicemail 9999
```

Pressing the messages button on the IP phone or dialing the voice-mail number will let you access the SSAM voice-mail system. You may configure “voicemail 9999” in telephony-service configuration mode.



Note

You must configure the voice-mail number 9999 in IP Telephony System in the **SAS > SSAM > Main > System** parameter.

Configure Call Forwarding to Voice Mail

```
ephone-dn 1
 number 1011
 call-forward busy 9001
 call-forward noan 9001 timeout 10
 call-forward all 9002

ephone-dn 2
 number 1012
 call-forward busy 9002
 call-forward noan 9002 timeout 10

! or
! call-forward all 9002
```

In this example 1011 is forwarded to 9001, and 1012 to 9002 when busy/noan/all.

Configure MWI

The SAS/SSAM voice mail is able to communicate MWI status with the Cisco CME router so that the Cisco CME router can signal the IP phone to turn the MWI lamp on and off. The MWI information is embedded in the called party’s telephone number 8000*....*1 or 8000*....*2. The target extension number is extracted from the called number digits that correspond to the “.” wildcard digits in the ephone-dn primary/secondary numbers.

```
ephone-dn 11
 number 8000*....*1 secondary 8000*....*2
 mwi on-off
```

In the above example, a call to 8000*1011*1 will turn MWI on for extension 1011, and a call to 8000*1011*2 will turn MWI off for extension 1011.

It is recommended that you configure 2, 4, 8 ephone-dns for MWI on and off if a 2-, 4-, 8-port SSAM is installed, respectively.

Configuration Example

The following example shows how to configure Cisco CME 3.0 to enable call forward (no answer/busy), direct access to the SSAM and MWI for a 4-port SSAM:

```
dial-peer voice 100 voip
 destination-pattern 9...
 session target ipv4:172.19.153.120
 dtmf-relay h245-alphanumeric
 codec g711ulaw
```

```

telephony-service
.
.
.
ip source-address 10.1.1.1 port 2000
create cnf-files
voicemail 9999

ephone-dn 1
number 1011
call-forward busy 9001
call-forward noan 9001 timeout 10
.
.
.
ephone-dn 11
number 8000*....*1 secondary 8000*....*2
mwi on-off

ephone-dn 12
number 8000*....*1 secondary 8000*....*2
mwi on-off

ephone-dn 13
number 8000*....*1 secondary 8000*....*2
mwi on-off

ephone-dn 14
number 8000*....*1 secondary 8000*....*2
mwi on-off

ephone 1
username "user1" password user1
mac-address 000A.8A21.4EBE
button 1:1 2:2

ephone 2
username "user2" password user2
mac-address 000A.8A2C.8C9E
button 1:1 2:2

```

SIP Integration with Cisco Unity Express

Cisco CME also supports an integrated voice mail and auto attendant on a network module running Cisco Unity Express for Cisco 2600XM, Cisco 2691 and Cisco 3700 platforms as a solution for small offices. For design guidelines and configuration details, see the appropriate Cisco Unity Express design guides.

Voice-Mail Integration in a Centralized Environment

You can share a single Cisco Unity server located at a centralized environment in which multiple Cisco CME routers are deployed in the branch offices. This is a cost-effective way of providing voice-mail service by eliminating the need of having one voice-mail system for each Cisco CME system. However, in the Cisco Unity case where overlapping dial plans are not supported, the network dial plan needs to be carefully designed because the call setup is across multiple Cisco CME routers and voice-mail servers through H.323. The Cisco CME router co-located with the Cisco Unity at the central site communicates with the Cisco Unity server through SCCP and serves as an MWI-delay server and a

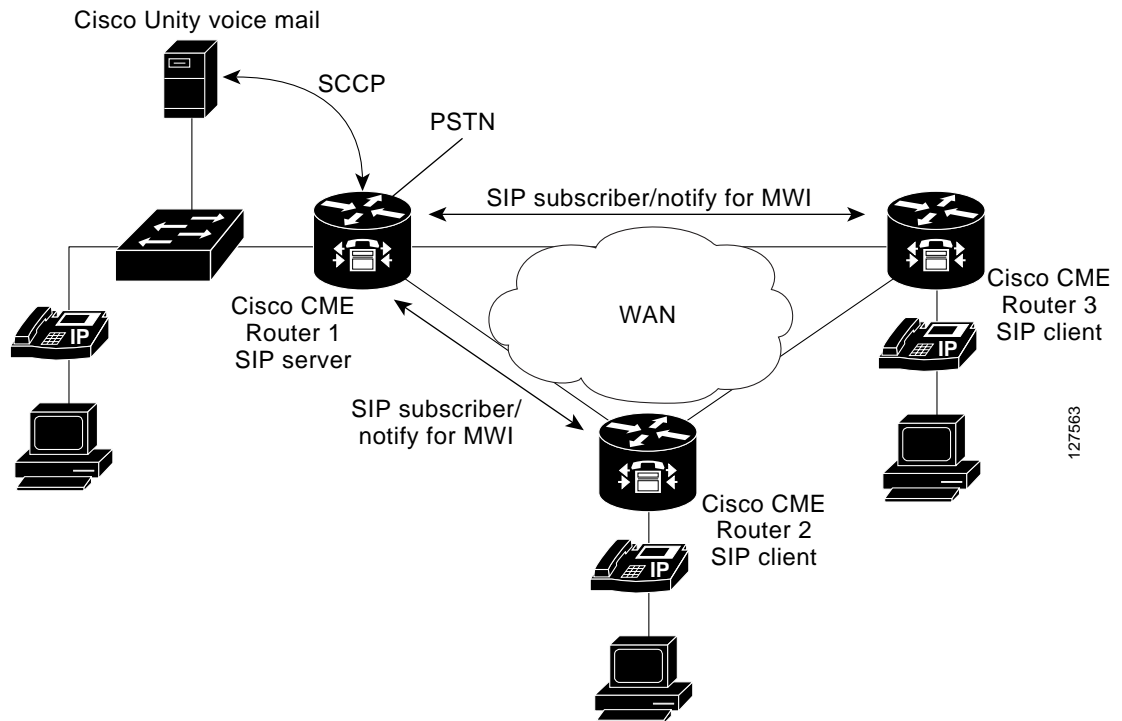
SIP-MWI notifier, while the other Cisco CME routers in the branch offices serve as MWI clients, sending subscribe messages and receiving notify messages to/from the MWI-relay server. Once the message is stored in the voice-mail system, the voice-mail system sends an MWI indication using SCCP by spoofing an IP phone appearance. If the extension is local, the Cisco CME attached to the voice-mail system sends an SCCP message to the lamp on the extension directly. If the extension is nonlocal, the Cisco CME system attached to the voice-mail system will relay it by using the SIP-MWI relay mechanism.

MWI Relay

The MWI relay method applies to a centralized environment in which a single voice-mail system is shared among multiple Cisco CME routers in remote branch offices. The SIP-MWI relay server running on the Cisco CME in the central site can act as a notifier to the other Cisco CME routers running as SIP-MWI relay clients and subscribers. The SIP-MWI relay server and clients communicate with each other through notify and subscribe messages. The Cisco CME running as the SIP MWI relay server can also be visualized as a proxy of a voice-mail system using SIP-MWI notify support. The central Cisco CME communicates with the Cisco Unity voice-mail system using SCCP messages. This is a cost-effective way of eliminating the need of having one voice-mail system for each Cisco CME.

Figure 14 shows how a Cisco Unity voice-mail system in the central site can be shared by multiple Cisco CME systems.

Figure 14 Cisco CME Voice-Mail Integration with Cisco Unity Server Using MWI Relay



The Cisco Unity voice-mail system sends the MWI status for an extension to Cisco CME Router 1. Cisco CME Router 1 does not find the extension locally so it sends a SIP Notify message, and the other Cisco CME Router 2 or 3 subscribing to the SIP messages can then signal the IP phone to turn the MWI lamp on/off upon receiving the messages for the phones connected locally.

The following is a configuration example for Cisco CME Router 1 shown in [Figure 14](#):

```
.
.
.
telephony-service
 ip source-address a.b.c.d
 mwi relay          ! Enables the router to relay the MWI information to the remote IP
 phones.
 mwi expires 99999 ! Sets the expire timer for registration for either the client
                  ! or the server.
 voicemail 52222
```

The following is an example configuration on Cisco CME Router 2 and Cisco CME Router 3 shown in [Figure 14](#):

```
.
.
.
telephony-service
.
.
.
 ip source-address e.f.g.h
 mwi sip-server a.b.c.d ! Subscribe to the SIP server on Cisco CME Router 1.
.
.
.
ephone-dn 1
 number 1000
 mwi sip          ! Needed for all the ephone-dns for MWI.
 call-forward noan 52222 time 10 ! 52222 is the Cisco Unity DN configured on
                               ! the CME-MWI server.

 call-forward busy 52222
```

The following configuration adds a VoIP dial peer on the Cisco CME SIP clients to reach 52222:

```
dial-peer voice xxxx voip
 destination-pattern xxxx
 session target ipv4:a.b.c.d
 codec g711u
 dtmf-relay h245-alpha
```

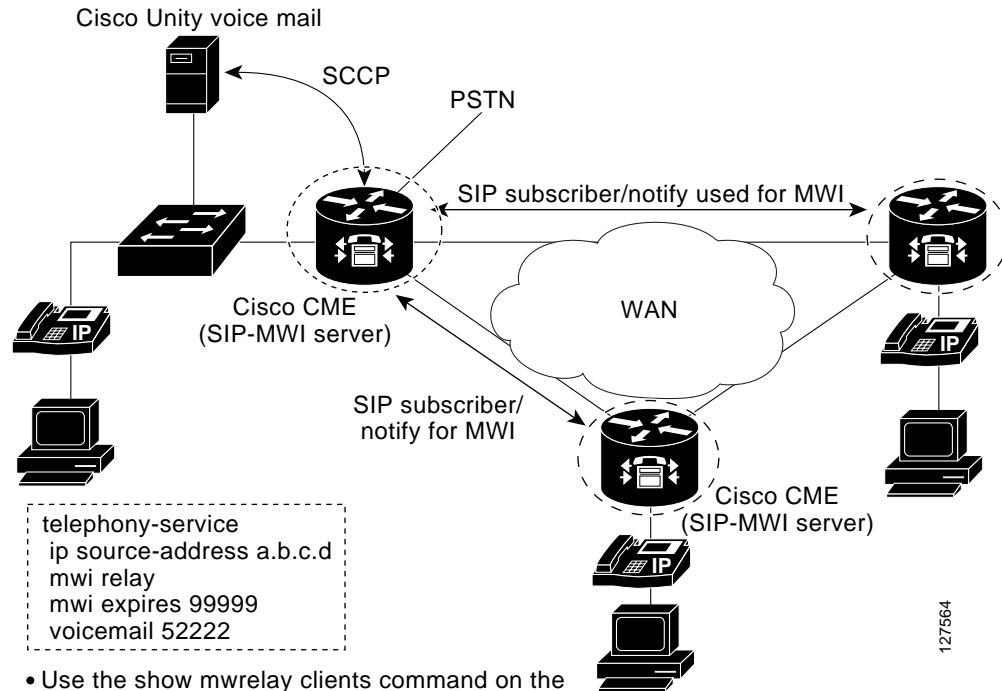


Note

To ensure that MWI works, the MWI status or Cisco Unity server must be resynced and restarted every time that a Cisco CME router is rebooted and reloaded.

[Figure 15](#) provides an overall illustration of this solution.

Figure 15 Cisco CME Voice-Mail Integration with a Cisco Unity Server (SIP MWI Server and Clients)



- Use the show mwrelay clients command on the Cisco CME SIP server to verify MWI registration.
- Use the addvoipdial peer command on the Cisco CME SIP clients for NTS.

```

dial-peer voice xxxx voip
destination-pattern xxxx
session target ipv4:a.b.c.d
codec g711u
dtmf-relay h245-alpha

telephony-service
ip source-address e.f.g.h
mwi sip-server a.b.c.d.
ephone-dn1
number 1000
mwi sip ! Needed for all ephone-dns for MWI
call-forward noan xxx time 10
! xxx is the Cisco Unity DN configured on the Cisco CME-MWI server
call-forward busy xxxx
    
```

**Note**

- On the Cisco Unity server, you need to configure either the 5-digit extension or the full E.164 number.
- Each IP phone needs a voice-mail account on the Cisco Unity server.
- When the Cisco CME is reloaded, the MWI information is lost. Therefore the administrator needs to resynchronize the MWIs by invoking the resync function on Cisco Unity.
- When reloaded, the SIP client does not subscribe back to the SIP server until after minimum of 600 seconds, which can be configured under the telephony-service.

Provisioning and Network Management for Cisco CME

This section provides information about the following topics:

- [Auto Registration, page 42](#)
- [Setup Utility, page 43](#)
- [Cisco CME GUI, page 43](#)
- [Syslog Messages and MIBs, page 44](#)
- [Billing Support, page 45](#)
- [AXL/SOAP APIs for Network Monitoring and Configuration Changes, page 45](#)

Auto Registration

Cisco CME 3.0 can automatically detect and register the new IP phones added to the network. You no longer need to configure or assign a MAC address to an IP phone. The newly added or installed IP phones will automatically get registered and perhaps get an assigned extension number if there is a pool of extension numbers preconfigured and available to use on a first come first serve basis. The following example configuration shows the setup of a pool of extension numbers for new phones:

```
telephony-service
  auto assign 1 to 8 type 7960 call-forward 59000 timeout 10
  create cnf-files

ephone-dn 1
  number 59001

ephone-dn 8
  number 59008
```

If the above is not configured in Cisco CME, the newly added IP phones will complete the boot and registration process without having any buttons associated with extension numbers (ephone-dns), and they will be unable to start making or receiving a call.

Use the above configuration when you need IP phones to be automatically registered or configured.

**Note**

You cannot automatically create a shared-line appearance on multiple phones by using the above configuration, nor is this configuration supported on the Cisco IP Phone 7914 Expansion Model.

Setup Utility

The Cisco CME setup tool provides a question-and-answer interface that allows you to set up an entire Cisco CME system at one time. This tool is extremely useful when you set up or install Cisco CME for the first time. You will be asked a series of questions, and based on your answers and selections, Cisco CME will automatically build a configuration file. If a previous Cisco CME configuration exists, you must configure the **no telephony-service** command to remove the existing configuration details, and then the setup tool can create a new set of commands for you. The following is a list of fields in the questions. You must answer all of the questions before the Cisco CME system can automatically build a configuration.

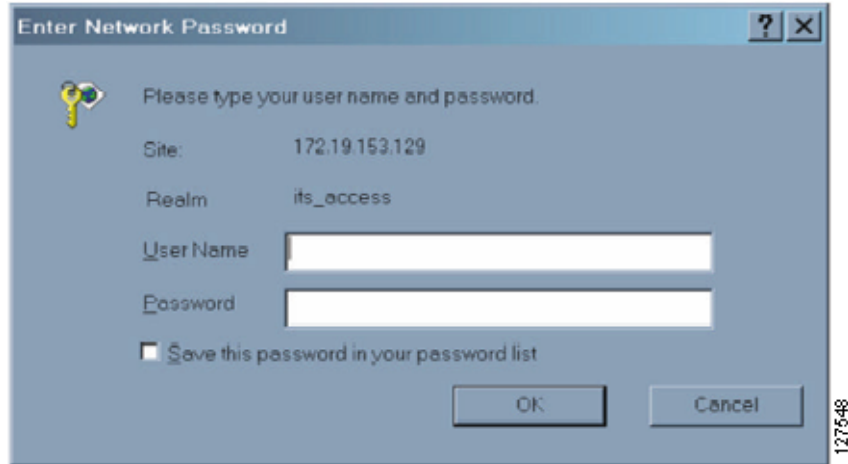
- DHCP service
- IP source address
- Number of phones
- PBX or key-switch mode
- Language
- Call progress tones
- First extension number
- DID service
- Full public telephone number
- Forward calls
- Voice mail number

Cisco CME GUI

You may use the Cisco CME GUI to configure the phones, ephone-dns, and some of the Cisco CME 3.0 features. The Cisco CME 3.0 GUI enhances the existing GUI with a consistent look and feel with Cisco Unity Express. The Cisco CME 3.0 GUI also adds some drop-down menus and provides several performance and usability enhancements. The Cisco CME GUI can be used for system administration or customer administration to create/modify/delete an extension or IP phone, phone lines, and speed dials. See the [Cisco CallManager Express 3.0 System Administrator Guide](#) for information about how to set up and configure the Cisco CME GUI and how to configure features for customer administration users.

Cisco CME 3.0 also supports HTTP 1.1 by using the pop-up box for authentication (see [Figure 16](#)). “Logon for Admin” and “system admin users” uses Authentication, Authorization, and Accounting (AAA), while normal user logon is still clear-text based.

Figure 16 Cisco IOS Telephony Services Engine Window



Syslog Messages and MIBs

Another network management feature that Cisco CME 3.0 has introduced is type 6 syslog messages, as shown below for IP phone registration and registration removal. The following syslog messages are useful for the central network management systems to manage Cisco CME and IP phones:

- %IPPHONE-6-REG_ALARM
- %IPPHONE-6-REGISTER
- %IPPHONE-6-REGISTER_NEW
- %IPPHONE-6-UNREGISTER_ABNORMAL
- %IPPHONE-6-REGISTER_NORMAL

You can enable Cisco IOS software to log all the syslog events into the buffer of the Cisco CME router and send syslog messages to a syslog server for management:

```
Router (config)# service timestamps log datetime msec localtime
Router (config)# aaa new-model
Router (config)# aaa authentication login default none
Router (config)# aaa accounting connection H.323 start-stop radius
Router (config)# gw-accounting syslog
Router (config)# logging 172.19.153.129 ! 172.19.153.129 is the ip address of the syslog
                                         ! server; multiple servers may also be specified.
```

To synchronize the Cisco CME to an external NTP server, configure the following, where the *ip-address* argument is that of the time server, which provides the clock synchronization:

```
Router (config)# ntp server ip-address
```

If there is no external NTP time source, use the internal clock as the time source using the following configuration:

```
Router (config)# ntp master
```

To ensure that the time stamps are correct, the router clock should be set to the correct time; an example configuration:

```
Router (config)# clock set 15:15:00 May 31 2001
```

Multiple syslog servers can be specified for redundancy on a heavily used network because syslog uses UDP as the underlying transport mechanism and data packets are unsequenced and unacknowledged.

Network management systems can also retrieve CDR and call history information from the following MIBs that Cisco CME leverages from Cisco IOS software:

- Cisco-DIAL-CONTROL-MIB (CDR/call history)
- Cisco-VOICE-CONTROL-MIB (extends to telephony and VoIP dial-peers call-legs)
- Cisco-VOICE-IF-MIB

Billing Support

Cisco CME 3.0 adds an Account Code field into the CDR records that can then be used by a RADIUS server or customer billing server for billing process. A soft key “Acct” is added to the Cisco IP Phone 7940 and Cisco IP Phone 7960, so that users can enter account codes from an IP phone during call alerting or connected state. This account code is also added into Cisco-VOICE-DIAL-CONTROL-MIB.

The following Account Code can be viewed in **show call active voice** command log:

```
Router# show call active voice
```

```
.
.
.
Telephony call-legs: 2
SIP call-legs: 0
H.323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 2
```

```
GENERIC:
SetupTime=97147870 ms
Index=1
PeerAddress=2001
```

```
.
.
.
TELE:
.
.
.
AccountCode 0100
.
.
.
```



Note

This Account Code field can also be added to the vendor-specific attribute fields for CDRs.

AXL/SOAP APIs for Network Monitoring and Configuration Changes

This section provides information on the following topics:

- [About AXL and SOAP, page 46](#)
- [Test AXL and SOAP Interface, page 47](#)

- [Poll AXL and SOAP Requests from a Network Management Station, page 47](#)
- [Deploying Cisco CME into Managed Service Providers, page 47](#)

About AXL and SOAP

The Cisco AVVID XML Layer (AXL) application programming interface (API) provides a mechanism for inserting, retrieving, updating, and removing data from the database using an XML Simple Object Access Protocol (SOAP) interface. The AXL API allows a programmer to access Cisco CallManager data using XML and receive the data in XML form, instead of using a binary library or DLL. The AXL API methods, known as “requests,” are performed using a combination of HTTP and SOAP. SOAP is an XML remote procedure-call protocol. Users perform requests by sending XML data to the Cisco CallManager server. The server then returns the AXL response, which is also a SOAP message.

Cisco CME 3.0 provides the XML APIs for IP phone and extension monitoring and configuration changes by extending the AXL/SOAP capabilities. AXL/SOAP APIs are used to poll the Cisco CME network elements that are the IP phones and ephone-dns/extensions from a network management system. Similar to AXL, communication between a network management system and a Cisco CME system is based on HTTP, and data exchange can only be initiated by polling from the network management system. However, Cisco CME can enable or disable the sending of data and configure control polling intervals.

The following is a list of XML APIs supported by Cisco CME 3.0 for monitoring:

- Get Static Information
 - IsgetGlobal—Get global information.
 - IsgetDevice—Get device information.
 - IsgetExtension—Get extension information.
- Get Dynamic Information
 - IsgetEvtCounts—Get number of events recorded in buffer.
 - IsgetDevEvts—Get device events (if IP phones are in the following states: register/unregister/decease).
 - IsgetExtEvts—Get extension events (virtual voice port up/down).

The following is a list of configuration commands supported by Cisco CME 3.0:

- **call application voice (IVR)**
- **dial-peer voice**
- **ephone**
- **ephone-dn**
- **ephone-hunt**
- **telephony-service**
- **vm-integration**

Test AXL and SOAP Interface

Cisco CME 3.0 provides a test program, `xml-test.html` (see [Appendix: XML Test Program APIs, page 57](#)), for users to verify if the Cisco CME router is set up correctly to respond to the AXL and SOAP requests. The following are the steps:

-
- Step 1** Load `xml-test.html` into flash memory.
- Step 2** Configure the following on the Cisco CME router:
- `ip http server`
 - `ip http path:flash`
 - `telephony-service mode`
 - `log password abcd`
 - `xmltest`
- Step 3** Type the following URL in the browser: `http://<ip-address of router>/ISApi/AXL/V1/soapisapi.is`.
- Step 4** When the Login window appears, log in as follows:
- username: any non-empty string
 - password: `abcd`
- Step 5** Select an API, enter the required information, and click the button next to it. After the XML request has been written to a form, go to the bottom of the page and click the Submit button.
- Step 6** If you get any error messages, the following debug on the router will help:
- `debug ip http appinout`
 - `debug ip http appdetail`
-

Poll AXL and SOAP Requests from a Network Management Station

The `xml-test.html` test program checks if the Cisco CME router can respond the AXL and SOAP requests. If you have it enabled, and if you are polling from an application of a network management station, you must disable the test program.

```
telephony-service
no xmltest
```



Note Polling requests from a network management system must be sent in clear text format.

Deploying Cisco CME into Managed Service Providers

Configuring or provisioning Cisco CME for a large number of Cisco CME routers is possible with the use of Cisco IE 2100, a network appliance. To do this, you put the configuration templates into the IE 2100 server, which will push the configuration templates to the Cisco CME servers globally.

AA with TCL and VxML

This section provides information on the following topics:

- [AA with Tcl IVR, page 48](#)
- [AA with VoiceXML, page 50](#)

AA with Tcl IVR

Cisco CME supports an AA using the Cisco IOS Tcl IVR 2.0 infrastructure. With AA configured and enabled on the Cisco CME router, inbound/outbound callers to the phones connected to the Cisco CME router can hear prompts, enter digits, and place calls. The AA mechanism is supported in the following scenarios:

- Inbound calls on FXO/PRI ports
- Outbound calls on FXS ports including analog phones configured through POTS
- Outbound calls on IP phones configured through ephone-dns—virtual FXS ports
- Inbound calls on VoIP dial peers



Note

- Tcl IVR 2.0 is Tcl-based scripting with a proprietary Cisco API. It provides extensive call control capabilities, signaling, and GTD manipulation.
- You can have as many concurrent IVR sessions as the number of calls for which the gateway or interface is rated. There is no limitation on multiple calls invoking the same Tcl script. However, the Cisco 3640 supports only 30 prompt payouts. The 31st prompt payout will be delayed until one of the earlier prompts finishes. There is a distinction between the number of simultaneous prompts that you can play and the number of simultaneous Tcl IVR calls that the gateway can handle. You will still be able to accept the 31st call; it is just that the prompt payout will be delayed until one of the other 30 prompt payouts is completed.

Requirements

Supported Platforms

The IVR AA is supported on the following platforms:

- Cisco 1751 and Cisco 1760 routers
- Cisco 2600 series routers
- Cisco 3600 series router (Cisco 3620, Cisco 3640, and Cisco 3660 routers)
- Cisco 3700 series router

Prerequisites

- Establish a working IP network.
- Configure Cisco CME and VoIP dial peers. For information on configuring Cisco CME, see the “[Configuring Dial Plans, Dial Peers, and Digit Manipulation](#)” chapter of the *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*. For information about configuring VoIP, see the *Voice over IP Software Configuration Guide* for the appropriate access platform.

- Configure a TFTP sever to perform storage and retrieval of the audio files, which are required by IVR AAs that must use Tcl IVR scripts and audio files.
- Write a Tcl script or modify the sample scripts provided in this documentation. The script can be stored on the TFTP server or in flash memory.
- The IVR prompts require audio file (.au) format of 8-bit, mu-law, and 8 KHz encoding. Cisco recommends the use of the following two audio tools or tools of comparable quality:
 - Cool Edit, a Windows application by Syntrillium Software Corp.
 - AudioTool, a Solaris application by Sun Microsystems Inc.
- Preload IVR prompts to flash/slot0, a TFTP/FTP server, or an external (RTSP-capable) server.



Note Some platforms may not support RTSP-based prompts.

- Ensure that your access platform and Cisco CME have a minimum of 32 MB of flash memory and 96 MB of DRAM memory.
- Configure and run the IVR application.
- Configure the router to run the Tcl IVR application and the script.

Configuring AA

The required tasks for configuring an AA include the following:

- Configure the Tcl IVR application.

```
call application voice appname tftp://dirt/lxia/ivr/CME_Cisco.2.0.0.0.tcl
call application voice appname operator 52222
call application voice appname aa-pilot 10228
call application voice appname language 1 en
call application voice appname set-location en 0
tftp://dirt/sanantha/GrandSlam/vespa2/
```

If the script and prompts are in flash memory, replace `tftp://dirt/sanantha/GrandSlam/vespa2/` with `flash memory:CME_Cisco.2.0.0.0.tcl`.

```
call application voice vespa flash:CME_Cisco.2.0.0.0.tcl
call application voice vespa operator 52222
call application voice vespa aa-pilot 10228
call application voice vespa language 1 en
call application voice vespa set-location en 0 flash:
```

- Configure the IVR AA for the PRI port.

```
dial-peer voice 5001 pots
  application appname
  incoming called-number 10228
  port 2/1:23          ! For PRI port 2/1
  forward-digits all
```

- Configure the IVR AA for the FXO port.

```
dial-peer voice 5002 pots
  application appname
  port 2/0/0 ! For FXO port 2/0/0
```

- Configure IVR AA for an FXS port.

```
dial-peer voice 3001 pots ! For an analog phone
  application appname
  destination-pattern 3001
  port 3/1/1
```

- Configure the IVR AA for a VoIP dial peer.

```
dial-peer voice 4001 voip
  application appname
  destination-pattern 41..
  session target ipv4:10.1.1.2
  dtmf-relay h245-alphanumeric
  codec g711ulaw
```

- Configure the IVR AA for an IP phone.

```
ephone-dn 1
  number 2493

ephone-dn 3      ! For an IP phone
  number 2493
  name "2493"
  application appname

ephone 1
  button 1:1 2:3 ! To hear the prompt when lifting up the handset and pressing button 3
```

- Run the IVR application

```
Router# call application voice load appname ! To reload the selected TCL script
```



Note

Signature checking from all platforms and the “test voip scripts” have been removed since Cisco IOS Release 12.2(11)T.

Tcl Developer Support

Cisco CME is shipped with a sample Tcl script and some prerecorded prompts for some basic AA functionality.

The sample script and prompts are packaged in a Cisco CME file and are downloadable from CCO at <http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key>.

For script customization, join the Cisco Developer Support Program. This program was created to provide you with a consistent level of support that you can depend on while leveraging Cisco interfaces in your development projects. A signed Developer Support Agreement is required to participate in this program. For more details, and to access this agreement, go to <http://www.cisco.com/go/developersupport> or contact developer-support@cisco.com.

See also the *Cisco TCL IVR and VoiceXML Application Guide* at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm>.

AA with VoiceXML

Cisco CME can leverage the Cisco IOS VoiceXML infrastructure to provide IVR AA features and call-control functionality such as call forwarding and conference calling.

**Note**

VoiceXML is a standard-based markup language for voice browsers. Existing web server and application logic can be used for VoiceXML applications, requiring less time and money to build infrastructure and perform development than traditional proprietary IVR systems require.

Requirements

VoiceXML is supported on the Cisco CME supported platforms Cisco 3640 and Cisco 3660 with Cisco IOS Release 12.2(11)T, and with 96 MB and 256 MB of DRAM, respectively.

Configuring AA with VoiceXML

To configure the Cisco CME router to run the script, you may do the following:

```
call application voice vxml_aa flash:simpleCall.vxml

dial-peer voice 11111 voip
  application vxml_aa
  incoming called-number 11111
  destination-pattern 11111
  session target ipv4:172.19.153.110
  dtmf-relay h245-signal
  codec g711ulaw
```

You may dial 11111 to hear the prompts and then enter digits.

VxML Developer Support

For information about VxML developer support, see

http://www.cisco.com/cgi-bin/dev_support/access_level/products.cgi?product=VOICE_XML_GATEWAY.

Cisco CME with NAT/Cisco IOS Firewall

This section provides information on the following topics:

- [Cisco CME with NAT, page 51](#)
- [Cisco CME with Cisco IOS Firewall, page 52](#)

Cisco CME with NAT

The Cisco CME router's LAN interface (Ethernet interface) is used as a source IP address that IP phones and the Cisco CME router communicate with. The IP addresses of the IP phones are internal addresses to the Cisco CME router and are in a different segment that is not visible by the external devices or callers. Other devices, including Cisco IOS gateways or gatekeeper, use the Cisco CME router's IP address to communicate instead of directly communicating with the IP phones. The Cisco CME router translates IP addresses back and forth for the traffic to route to the IP phones or outside of the network area. Therefore, no Network Address Translation (NAT) configuration is needed when talking to the IP phones locally attached to the Cisco CME router. However, when IP phones need to talk to other devices outside the firewall of the Cisco CME network, you must to configure NAT on the Cisco CME router.

Cisco CME with Cisco IOS Firewall

The Cisco IOS firewall, running on Cisco IOS routers, provides a network-based firewall solution with the functionality of context-based access control (CBAC), Intrusion Detection System (IDS), authentication proxy, and URL filtering. A firewall provides access-control between internal and external networks. It identifies networks as “inside” (private) or “outside” (public) in which packets can get from inside to outside, blocked by default from outside to inside, and packets associated with an inside-originated connection are allowed to pass in. Many firewalls work only if all outside traffic originates from well-known sockets and do not handle asymmetric traffic, such as UDP media. Cisco IOS firewalls allow the packets/traffic to pass through on the basis of their source and destination IP addresses and the configured firewall policy.

Cisco CME is a software feature added to the Cisco IOS routers that provides call processing for IP phones using SCCP for branch and SMB in a managed service provider environment. There will be cases in SMB and branch offices where only one router is available to provide Internet access and IP telephony service. Cisco CME requires that all IP phones attach to the Cisco CME router locally. Thus SCCP support on the Cisco IOS firewall is needed for locally generated SCCP traffic.

Problems on Cisco CME with Cisco IOS Firewall

SCCP is a Cisco-proprietary small version of H.323. H.323 traffic can be classified into call signaling, call control, and media communication. H.323 uses Q.931, H.225, and H.245 to set up, manage and control, and tear down calls. When Cisco CME with H.323 and SCCP protocols are run, you must consider how signaling and media streams are affected by the Cisco IOS firewall.

Signaling Stream

An H.323 call requires a TCP connection for H.245 signaling that does not have a well-known port associated with it. The H.245 port is dynamically assigned. Because this port is not known ahead of time and cannot be configured when defining firewall policy, the Cisco IOS firewall will block the H.245 message and the call signaling procedure will fail. When NAT is used in the H.323 signaling path, an inside IP address (behind NAT), not known to the rest of the world, will be used as the “calling party” information element in the H.225 signaling stream; thus an incoming call that attempts to make an H.225 connection back to that address will fail.

Media Streams (RTP Streams)

Real-time transport protocol (RTP) streams run on top of User Datagram Protocol (UDP) and do not have any associated fixed ports. Each type of media stream has one or more channels with dynamically assigned source/destination/port numbers, which are neither known ahead of time nor able to be preconfigured in the firewall policy. For the media stream to traverse the firewall, the firewall needs to open many UDP ports with source and destination pairs for each call session, thus inducing vulnerabilities to the network behind the firewall.

Because the Cisco IOS firewall does not allow outside traffic to transverse to the inside, VoIP calls (inbound calls) will fail. Furthermore, dynamic RTP/RTCP ports used by the endpoints are not automatically opened and allowed without modification of the security policy. The problems are summarized as follows:

- The firewall only looks at Layer 3 addresses.
- VoIP signaling protocols embed IP addresses at a layer:
 - RTP/RTCP works at Layer 5.
 - By default, firewalls do not allow outside to inside traffic.

- The Cisco IOS firewall feature set and NAT and PIX have application functionality called Application Layer GW (ALG) or fix-up protocol, which helps in resolving these issues.
- The VoIP application is composed of a dynamic set of protocols that include the following:
 - SIP, MGCP, H.323, and SCCP for signaling.
 - SDP, H.225, and H.245 for capability exchange.
 - RTP/RTCP for control and audio media. RTP/RTCP both use a dynamic port for the audio media ranging from 16384 to 32767 for all Cisco products

The caveat CSCdx39135 was opened to track and resolve the problem.

Current Status

Currently, the Cisco IOS firewall does not support SCCP inspection because outgoing packets will be converted to H.323 or SIP, and thus there is no need for SCCP inspection. However for incoming SCCP packets inspection, you can use access control lists (ACLs) to filter out unwanted packets or traffic. However, the Cisco IOS firewall will add inspection support for any locally generated traffic as a fix for caveat CSCdx39135.

Workaround

The following are four alternative solutions to provide security to Cisco CME users:

- Run the Cisco IOS firewall on a different router.
- Set up max-connections in Cisco CME. This is available with the regular H.323 implementation in Cisco IOS software and can help control the maximum number of H.323 (H.225 setup Inbound+Outbound) calls that will be processed.
- Set up ACLs to accept H.225 connections only from the gatekeeper if the gatekeeper in the network is of routed signaling type.
- Use H.235 security to authenticate the callers and provide additional call security.

Troubleshooting Cisco CME Features

This section provides information on the following topics:

- [Troubleshooting Cisco CME Commands, page 53](#)
- [Cisco CME Caveats, page 55](#)

Troubleshooting Cisco CME Commands

- The **show ephone** commands include the following:
 - **show ephone 7910**
 - **show ephone 7940**
 - **show ephone 7960**
 - **show ephone H.H.H**
 - **show ephone offhook**

- **show ephone registered**
- **show ephone remote**
- **show ephone ringing**
- **show ephone summary**
- **show ephone tapclients**
- **show ephone telephone-numbers**
- **show ephone unregistered**
- The **show telephony-service** commands include the following:
 - **show ephone-dn**
 - **show ephone-dn loopback**
 - **show ephone-dn summary**
 - **show telephony-service admin**
 - **show telephony-service all**
 - **show telephony-service dial-peer**
 - **show telephony-service ephone**
 - **show telephony-service ephone-dn**
 - **show telephony-service voice-port**
- The **debug ephone** commands include the following:
 - **debug ephone alarm**
 - **debug ephone detail**
 - **debug ephone error**
 - **debug ephone keepalive**
 - **debug ephone loopback**
 - **debug ephone moh**
 - **debug ephone mwi**
 - **debug ephone pak**
 - **debug ephone raw**
 - **debug ephone register**
 - **debug ephone state**
 - **debug ephone statistics**
- To debug call transfer and forward related problems, use the following commands:
 - **debug voice ccapi inout**
 - **debug voice ivr all**
 - **debug vtsp tone**
- Troubleshooting voice-mail integrations (SIP) and MWI commands include the following:
 - **debug ccsip all**
 - **debug ccsip messages**
 - **debug ephone detail**

- **debug ephone error**
- **debug ephone mwi**
- **debug ephone statistics**
- **debug ephone-dn mwi**
- **show mwi relay clients** (CME SIP server to check if DN's are registered for MWI)
- **debug mwi relay events**
- To show SIP messages sent and received, use the following commands. These commands display the status of all current registrations.
 - **show sip-ua register status**
 - **show sip-ua register status secondary**

Cisco CME Caveats

- The AA script handoff to the H.450 call transfer script and the Cisco CME 3.0 built-in call transfer code do not work.
- Cisco CME voice-mail integration with Cisco Unity SIP is still in progress and is an on-going effort.
- Full Cisco CME 3.0 call feature support on the Cisco IP Phone 7902, Cisco IP Phone 7905G and Cisco IP Phone 7912G is delayed pending new phone firmware availability. This affects call pickup, DND, login, flash memory, and account code support.
- Cisco CME 3.0 supports only English with the Cisco IP Phone 7905G and Cisco IP Phone 7912G. There is no language issue with the Cisco IP Phone 7902 because it does not have a display.
- The Cisco 3745 crashes on call transfer between PRI and BRI (CSCeb11681).

Additional References

- [Related Documents, page 55](#)
- [Standards, page 57](#)
- [MIBs, page 57](#)
- [RFCs, page 57](#)

Related Documents

Related Topic	Document Title
Cisco CME 3.0 configuration and IP phone user and quick reference cards	<ul style="list-style-type: none"> • See the Cisco CME feature guides at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_feature_guide09186a0080189132.html.
Cisco SRST 3.0 configuration and IP phone quick reference cards	<ul style="list-style-type: none"> • See the Cisco SRST 3.0 feature guides at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_feature_guide09186a008018912f.html.

Additional References

Related Topic	Document Title
Cisco IP phones administration, installation, and regulatory information	<ul style="list-style-type: none"> • Cisco IP Phones and Services
Cisco Unity Express technical documentation	<ul style="list-style-type: none"> • Cisco Unity Express Documentation Roadmap
Cisco Unity Express integration	<ul style="list-style-type: none"> • Integrating Cisco CallManager Express and Cisco Unity Express
Cisco Unity integration	<ul style="list-style-type: none"> • Cisco CallManager Express 3.0 Integration Guide for Cisco Unity 4.0
XML guidelines for Cisco IP phone services	<ul style="list-style-type: none"> • Cisco IP Phone Services Application Development Notes
XML application programming interface (API)	<ul style="list-style-type: none"> • XML Developer Guide for Cisco CME/SRST
TAPI development	<ul style="list-style-type: none"> • TAPI Developer Guide for Cisco CME/SRST
Default session application	<ul style="list-style-type: none"> • Default Session Application Enhancements, Cisco IOS Release 12.2(15)ZJ
Domain management with Cisco Packet Telephony Center - Virtual Switch (Cisco PTC - VS)	<ul style="list-style-type: none"> • Provisioning Manager - Managed Cisco CallManager Express Router
Dynamic Host Configuration Protocol (DHCP)	<ul style="list-style-type: none"> • Cisco IOS DHCP Server • “Configuring a DHCP Server” in the “Using Autoinstall and Setup” chapter in Part 1: “Cisco IOS User Interfaces” in the Cisco IOS Configuration Fundamentals and Network Management Configuration Guide
Dial peers, DID, and other dialing issues	<ul style="list-style-type: none"> • 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)
H.323	<ul style="list-style-type: none"> • Cisco IOS H.323 Configuration Guide
SIP	<ul style="list-style-type: none"> • Cisco IOS SIP Configuration Guide • SIP Gateway Enhancements, Cisco IOS Release 12.2(15)ZJ
ATAs	<ul style="list-style-type: none"> • Cisco ATA Release Notes
Additional Cisco IOS Voice Configuration Library documents, including library preface and glossary	<ul style="list-style-type: none"> • Cisco IOS Voice Configuration Library at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm
Cisco IOS command references	<ul style="list-style-type: none"> • Cisco IOS Debug Command Reference, Release 12.3T • Cisco IOS Voice Command Reference, Release 12.3T • Cisco CallManager Express 3.2 Command Reference
Cisco IOS troubleshooting information	<ul style="list-style-type: none"> • Cisco IOS Voice Troubleshooting and Monitoring Guide

Related Topic	Document Title
Cisco IOS configuration examples	<ul style="list-style-type: none"> Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html <p>Note From the website, select a technology category and subsequent hierarchy of subcategories, and then click Technical Documentation > Configuration Examples.</p>
Additional configuration guides	<ul style="list-style-type: none"> <i>Cisco IOS Voice Configuration Library</i> <i>Tcl IVR API Version 2.0 Programmer's Guide</i> <i>Cisco VoiceXML Programmer's Guide</i> <i>Stonevoice Application Suite SAS Configuration Guide</i> <i>Stonevoice Softswitch Answering Machine Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Appendix: XML Test Program APIs

The following are XML test program (xml-test.html) APIs:

ISgetGlobal [View XML]

Top of Form

Global

Bottom of Form

ISgetDevice [View XML]

Top of Form

DeviceID

DeviceName

Bottom of Form

ISgetExtension [View XML]

Top of Form

ExtensionID

ExtensionName

Bottom of Form

ISgetEvtCounts [View XML]

Top of Form

Events Count

Bottom of Form

ISgetDevEvts [View XML]

Top of Form

Dev Event ID

Dev ID

Dev Name

Bottom of Form

ISgetExtEvts [View XML]

Top of Form

Ext Event ID

Ext ID

Ext Name

Bottom of Form

ISsetKeyPhones [View XML]

Top of Form

Phone Name

Bottom of Form

ISexecCLI [\[View XML\]](#)

Top of Form

CLI-1

CLI-2

CLI-3

CLI-4

CLI-5

CLI-6

CLI-7

CLI-8

CLI-9

CLI-10

Bottom of Form
