Connecting Multiple Cisco Unified CallManager Express Systems with VoIP

This chapter describes the ways in which you can use Cisco Unified CallManager Express (Cisco Unified CME) as a component of a larger network using the two major Voice over IP (VoIP) protocols—H.323 and SIP—to link multiple Cisco Unified CME systems. It examines some of the considerations that apply within a networked environment that do not arise in simpler standalone configurations. This chapter focuses on the call handling implications of using Cisco Unified CME in a network.

The following sections address specific multiple Cisco Unified CME deployment issues:

Note For additional information, see the "Related Documents and References" section on page xii.

Considerations When Integrating Cisco Unified CME in H.323 and SIP VoIP Networks

H.323 is the dominant protocol deployed for VoIP networks from an installed-base perspective. Because H.323 is more mature than SIP, you can expect to see increased real-world interoperability between different vendors' H.323 products, particularly with basic call handling. However, many of the high-level VoIP networking considerations that apply to H.323 apply equally in the SIP context. Some technical and protocol-specific differences exist between H.323 and SIP VoIP networking, but for the most part, you'll find more commonality than difference, at least at the level of technical detail that this chapter addresses.

The shared aspects of the two protocols means that the overall high-level architecture and distribution of hardware and primary component roles within your VoIP network don't significantly depend on which protocol you choose to use for intersite VoIP. For networks built on either H.323 or SIP, you are dealing

with peer-to-peer communication between sites. Therefore, you also need some kind of telephone number directory system to be able to resolve the IP address of the appropriate destination VoIP peer device for intersite calls.

In contrast, this similarity between H.323 and SIP does not extend to Media Gateway Control Protocol (MGCP) (and also Skinny Client Control Protocol [SCCP]), which takes a significantly different approach to telephony. Of course, it is still possible to connect Cisco Unified CME to MGCP networks, primarily using either H.323 or SIP. Many MGCP Call Agent implementations (using MGCP internally for phone control) use H.323 or SIP to connect separate Call Agents (as intersystem peer-to-peer). Cisco Unified CME itself does not support control of MGCP endpoints. Cisco Unified CME uses SCCP for phone control, and SCCP shares many common traits with MGCP.

The term *VoIP* here specifically describes "long-distance" VoIP telephone calls that traverse a WAN. This interpretation excludes SCCP used to control local IP phones. Although SCCP technically does use VoIP technology, it is primarily used in the context of operating voice calls within the confines of a LAN with more or less unlimited bandwidth and many fewer concerns about security.

You can view the H.323/SIP versus SCCP contrast as the difference between interbranch office voice traffic and intrabranch office voice traffic, or alternatively as long distance (WAN) versus local VoIP (LAN). This division is useful in many ways, because it inherently supports the often-necessary difference in treatment of calls between internal and external phone users.

In some cases, you might want to treat H.323 calls as internal calls and not want a high degree of differentiation in the treatment of LAN versus WAN calls, such as calls between separate systems on two floors of the same building. Cisco Unified CME has features that address this, although currently you cannot treat a network of many Cisco Unified CME systems as if they are a single logical entity with full intersite feature transparency. Both H.323 and SIP still have obstacles to overcome before this is really possible. Not least of these are issues surrounding meaningful interoperability with another company's devices for services beyond basic calls.

When you extend VoIP calling into the WAN space, you might also have to consider the difference between VoIP calls that come from other Cisco Unified CME nodes within your WAN network versus VoIP calls that are from VoIP Public Switched Telephone Network (PSTN) gateways or even from other independent external/wholesale VoIP carrier networks. You can link independent VoIP networks together and into your corporate VoIP network using IP-to-IP gateways. This arrangement may be desirable if you want to obtain international and long-distance phone service directly from a carrier-class VoIP service provider and have this linked at the VoIP level to your private enterprise VoIP network.

Note For more information about Cisco IP-to-IP Gateway functionality, see the document at: http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_qanda_item09186a00801da69b.shtml

SIP potentially has some advantages over H.323 in terms of separating intersite VoIP calls from true external VoIP calls, because SIP uses the Internet concept of domains. It is a fair assumption that all of the intersite calls will use the same root domain name and that this fact can be used to make the required distinction. However, from a purely practical security point of view, you will probably want any truly external VoIP traffic entering your corporate VoIP network to pass through an IP-to-IP gateway and also a firewall, regardless of whether you choose to use SIP or H.323. This means that you should have the opportunity to appropriately classify and mark the external calls at the point of entry in either type of network.

Alternatively, you can keep your VoIP network entirely separate at the IP level and simply connect into VoIP service provider carrier networks through time-division multiplexing (TDM)-based PSTN-like gateways (at some cost in terms of increased end-to-end voice path delay). For the sake of simplicity and clarity, the rest of this chapter ignores the IP-to-IP possibility and includes only the PSTN gateway

scenario. For many reasons, what is on the far side of the gateway—whether PSTN or IP-to-IP—is not hugely significant. It's the gateway's job to take care of whatever adaptation is needed to provide the interconnection path.

Note When you configure SIP or H.323 on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.

Cisco Unified CME uses the standard ports summarized in Table 6-1 for call signaling, and media transport. The same ports are used by Cisco Unified CallManager and Cisco IOS voice gateway products.

Table 6-1 Cisco Unified CME VoIP Port Numbering

Protocol	Port Numbers	Port Type
H.225 (call signaling)	1720	TCP
SIP	5060	UDP/TCP
RTP	16384 to 32768	UDP (dynamic)
RTP (LAN)	2000	UDP
SCCP	2000	TCP
H.245	11000 to 11999	TCP (dynamic)
H.225 RAS	1719	UDP
Unicast GK Discovery	1718	UDP
Multicast GK Discovery	223.0.1.4	UDP

Integrating Cisco Unified CME in an H.323 Network

There are two basic approaches to connecting a Cisco Unified CME system to an H.323 network: the first uses no gatekeeper (GK), and the second does. A direct interconnection of sites with H.323 implies that each site must be knowledgeable about how to reach every other site. This works well in small networks of only a handful of nodes, but as the network grows larger, the configuration becomes increasingly cumbersome to maintain. In its simplest form, a gatekeeper is a device that provides a directory service that translates a telephone number into an IP address. Using a gatekeeper provides significant scalability by centralizing the interconnection of the individual sites so that each site needs to be aware of only the gatekeeper and not every other site in the network.

The following sections discuss different approaches to building H.323-based Cisco Unified CME networks:

- A Simple Two-Node Topology with H.323, page 6-5
- A Large Multinode Topology with H.323, page 6-7
- The Role of an H.323 Gatekeeper, page 6-9
- Public and Internal Phone Numbers in an H.323 Network, page 6-13
- Registering Individual Telephone Numbers with a Gatekeeper, page 6-15
- Internal and External Callers for VoIP, page 6-16

Rather than being alternative approaches, they represent a simpler approach for smaller networks with only a few nodes and a more scalable approach for larger multinode networks.

A Simple Two-Node Topology with H.323

In the simplest case, you can just connect two Cisco Unified CME systems via an IP-enabled serial data link (or Ethernet), and configure VoIP dial peers on each system to symmetrically direct calls that are destined for nonlocal extension numbers to the other Cisco Unified CME system. In other words, if the Cisco Unified CME recognizes that the extension number being dialed is not present in its internal list of phone numbers, it can assume that it should send the call to the other Cisco Unified CME, as shown in Figure 6-1.

Figure 6-1 Simple Two-Node Cisco Unified CME H.323 Network

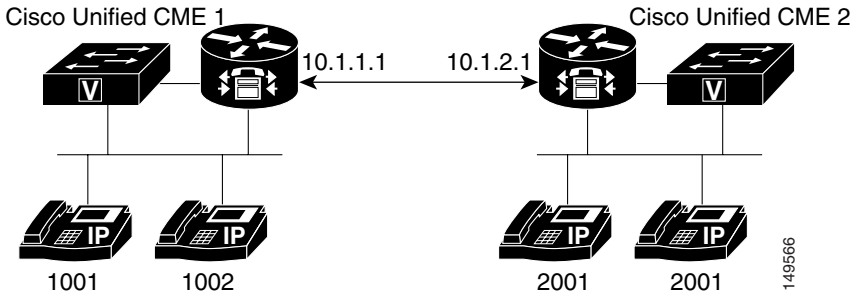
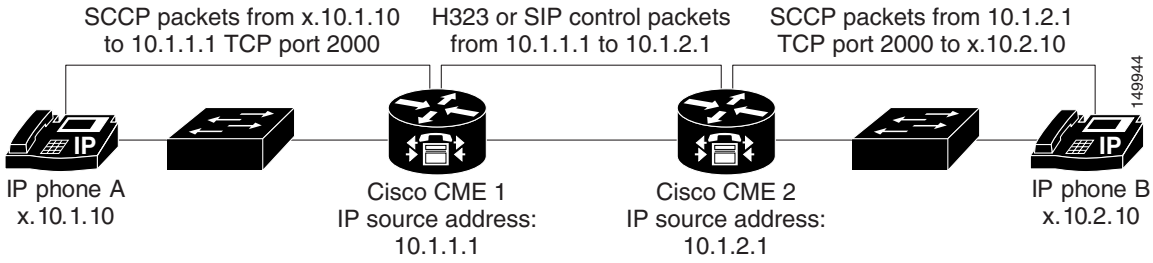


Figure 6-2 and Figure 6-3 present flow diagrams illustrating proxy behavior between Cisco Unified CME nodes in the two-node H.323 network illustrated in Figure 6-1.

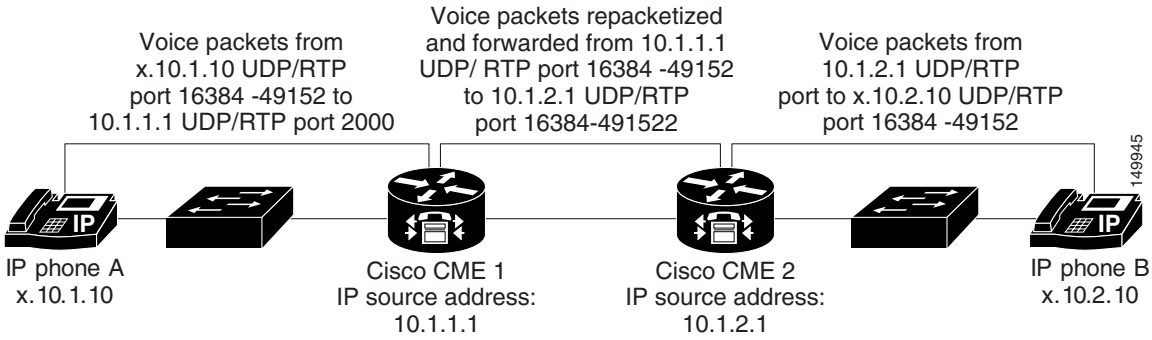
For VoIP across the WAN, all skinny and H.323 call control packets are proxied by the IP source address of the local Unified CME router. See Figure 6-2.

Figure 6-2 Cisco Unified CME VoIP Call Flow—Call Control Packet Proxy Behavior



After call signaling is established, RTP/UDP media traffic will be proxied by IP source address UDP/RTP port 2000 of the local Unified CME router. See Figure 6-3.

Figure 6-3 Cisco Unified CME VoIP Call Flow—RTP/UDP Traffic Proxy Behavior



The following examples show the relevant configuration extracts of the two systems. It shows a pair of Cisco Unified CME systems that have extensions 1000 to1099 on *Cisco Unified CME 1* (IP address 10.1.1.1) and 2000 to 2099 on *Cisco Unified CME 2* (IP address 10.1.2.1).

- Cisco Unified CME 1

```
dial-peer voice 2000 voip
     destination-pattern 20..
     session target 10.1.2.1
     dtmf-relay h245-alphanumeric
     codec g729r8
     no vad
telephony-service
ip source-address 10.1.1.1 port 2000
```

- Cisco Unified CME 2

```
dial-peer voice 1000 voip
     destination-pattern 10..
     session target 10.1.1.1
     dtmf-relay h245-alphanumeric
     codec g729r8
     no vad
telephony-service
ip source-address 10.1.2.1 port 2000
```

Note The **dtmf-relay** configuration portion of the output is explained in the "DTMF Relay for H.323" section on page 6-17.

You can use this simple symmetrical VoIP dial peer technique to join two Cisco Unified CME systems even within a single site to increase the total phone count supported beyond the capacity of a single Cisco Unified CME system. The downside of doing this is that it does not give you a truly monolithic system from a configuration, inter-Cisco Unified CME feature transparency, and management point of view. This arrangement requires you to administer the two systems separately, which may be acceptable if the two systems are split between naturally different and separate sections of your company (for example, administration and manufacturing).

This arrangement also limits the phone features you can use across the two systems. You can operate simple features such as call transfer and forwarding, and you can share a single voice mail device between systems, including inter-Cisco Unified CME distribution of message waiting indication (MWI). However, Cisco Unified CME does not support more advanced features, such as shared line and call pickup, across the H.323 or SIP interconnection.

One final point about this arrangement is that you can optionally choose to provide a physical PSTN connection on just one Cisco Unified CME system and have that Cisco Unified CME system also act as a VoIP PSTN gateway for the second Cisco Unified CME system.

Although this discussion considers H.323 and SIP "long-distance" protocols, the use of these protocols is not related to physical distance. You can use H.323 and SIP to link systems 1000 feet apart the same as you would link systems 1000 miles apart. This ability is one of the key advantages of VoIP technology over traditional TDM systems. With the appropriate IP infrastructure, you can link systems and users more or less independent of the physical distance that separates them. This means that you can give a remotely located Cisco Unified CME system a phone extension number and voice mailbox that appears to your phone users to belong to their local Cisco Unified CME system (with the aforementioned restriction on advanced phone feature operation between systems across VoIP). The historical out-of-area-code restrictions that apply to traditional TDM-based centrex phone systems largely do not apply in the VoIP context.

The one caveat in this area is the impact on access to public emergency services. Users dialing for emergency assistance (such as police, fire, or ambulance) should be routed into the PSTN via a PSTN connection that is local to their physical location. The calling party information provided to the PSTN connection and emergency services operator for this type of call must display an appropriate phone number (and therefore an associated physical location) that is within the emergency services area of the PSTN link being used.

A Large Multinode Topology with H.323

If you want to connect more than two Cisco Unified CME systems, you can extend the basic approach used to connect two systems and add a third, fourth, or more Cisco Unified CME systems—up to a point. For a low number of systems, such as five or six, it's usually possible to add VoIP dial peers to your Cisco Unified CME system that indicate the static IP address of the other system to reach. This is especially true if your dial plan is reasonably well segmented such that you can infer to which Cisco Unified CME system the call should be sent based on the first one or two digits of the dialed extension number. For example, Cisco Unified CME system 1 is given extension numbers 5000 to 5099, Cisco Unified CME system 2 is given extension numbers 5100 to 5199, and so on.

Even if your dial plan is not entirely evenly divided, you can still use this approach if you are prepared to build the necessary dial peer-based configuration. At the limit of this method, you can construct systems in which you create an individual H.323 VoIP dial peer on each Cisco Unified CME system for each remotely located extension number. You can follow this approach as far as available memory and your patience in creating and maintaining the configuration allow. As the number of dial peers increases, the post-dial delay increases somewhat, because the Cisco Unified CME system might need to search through a couple hundred dial peers to find the right information. In the very worst case, a network of five Cisco Unified CME systems with 20 extensions each would need 80 VoIP dial peers created (and maintained) on each system. That is assuming that your extension number distribution is fully random across the full set of Cisco Unified CME systems. Troubleshooting such a system in the event of misconfiguration is challenging, however.

Another drawback of the multiple dial peer configuration is that there is no good way to do call admission control (CAC) in order to prevent an excessive number of voice calls from trying to use the same WAN link at the same time. This can be an issue if your expected maximum call volume might be greater than the capacity of your WAN links. See the next section for more on this issue.

Cisco IOS software has a built-in CAC mechanism with the **call threshold** interface command. This feature limits both inbound calls and outbound calls for a specific interface on the Unified CME router once a maximum threshold has been exceeded. For example, the following command causes calls from GigabitEthernet0/0 to be rejected after the number of simultaneous inbound/outbound calls exceeds five. Calls are then allowed once the maximum number of simultaneous calls falls below 3.

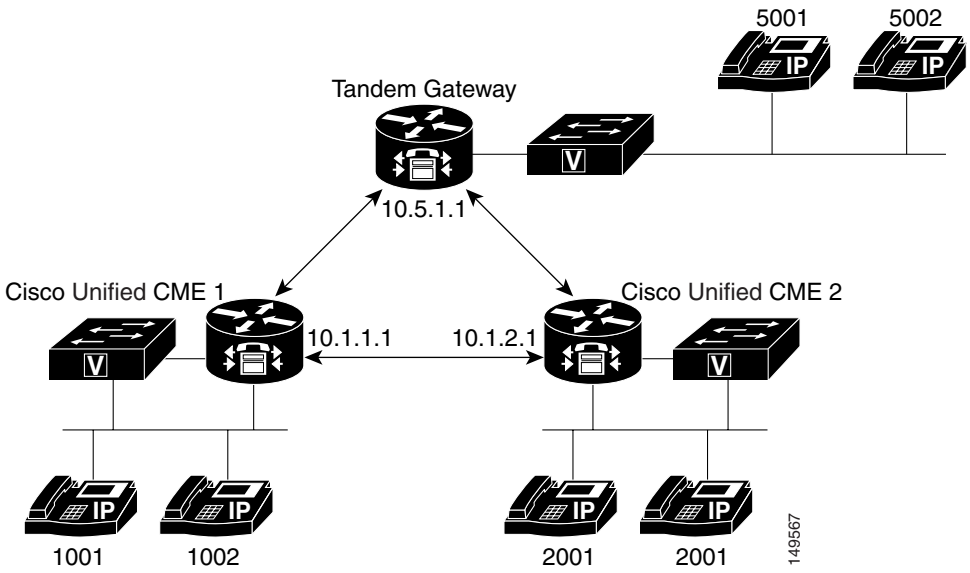
```
call threshold interface GigabitEthernet0/0 int-calls low 3 high 5
```

The benefit of this feature is that it does not require gatekeeping and can operate across multiple dial-peers. It is not subject to dial-peer maximum connection limitations. The limitation of this mechanism is that the maximum number of simultaneous calls is an aggregate of the total inbound and outbound calls. You cannot set up different thresholds for outbound or inbound calls using this mechanism.

Alternatively, you can use the VoIP Tandem Gateway feature of Cisco Unified CME 3.1 and above. This allows you to construct hub-and-spoke or hop-by-hop call routing arrangements. Hub-and-spoke call routing arrangements are historically common in small-scale voice over Frame Relay (VoFR) and voice over ATM (VoATM) networks. In these small-scale networks, you might have a single larger "hub" Cisco Unified CME system with approximately 100 users at a primary site, with perhaps five satellite Cisco Unified CME systems, each with 20 users linked on VoIP "spokes" to the primary. In this arrangement, only the central hub site needs VoIP dial peers to be configured to define the location of all network-wide extensions. The spoke satellite sites only need to know to send nonlocal calls to the hub site. The central hub site can then relay the call to the final spoke site destination.

This type of arrangement makes the most sense if the physical (Layer 1 and Layer 2) connectivity topology of your IP transport network mirrors the same hub-and-spoke arrangement as the dial plan. With this situation, IP packets that flow between different spoke sites inevitably get IP Layer 3 routed via the central hub site Cisco Unified CME router. The hub-and-spoke dial plan arrangement causes the VoIP calls and voice packets to get routed by the application layer instead, with relatively minor added delay, as shown in Figure 6-4.

Figure 6-4 Multinode Cisco Unified CME Tandem Gateway H.323 Network



The following example shows the relevant configurations of the nodes shown in the network.

- Cisco Unified CME 1

```
dial-peer voice 2345 voip
   destination-pattern [2345]0..
   session target ipv4:10.1.5.1
   no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1345 voip
```

```
   destination-pattern [1345]0..
   no vad
session target ipv4:10.1.5.1
```

- Tandem Gateway Node

```
voice service voip
   allow-connections h323 to h323
   dial-peer voice 1000 voip
      destination-pattern 10..
      session target ipv4:10.1.1.1
      no vad
   dial-peer voice 2000 voip
      destination-pattern 20..
      session target ipv4:10.1.2.1
      no vad
```

Using a single dial peer at the spoke sites to direct calls to the hub site and all far-end spoke sites beyond it also allows you to more easily use CAC per dial peer call-counting mechanism (which you'll learn more about in the following section). This is shown in Figure 6-4. You can use regular expressions in dial peer destination patterns. For example, if you need a single dial peer that references extensions in multiple ranges, such as 10xx, 30xx, 40xx, and 50xx (not including 20xx), you can use the following command:

destination-pattern [1345]0..

The values in square brackets ([ ]) provide a list of alternative values—in this case, 1, 3, 4, and 5. You can also use this to encompass a continuous range. For example, you can also write the preceding example as 1,3-5:

destination-pattern [13-5]0..

However, an even better and fundamentally more scalable approach to inter-Cisco Unified CME H.323 VoIP call routing is to use an H.323 GK (as you will see in the next section). This is the most practical approach to link tens or hundreds of Cisco Unified CME systems.

The Role of an H.323 Gatekeeper

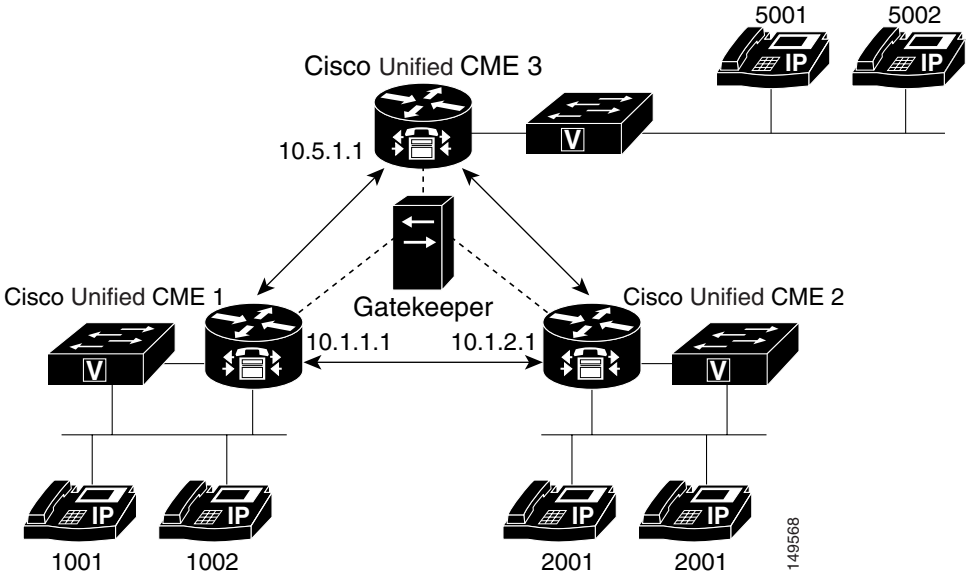
The primary role of an H.323 gatekeeper is to provide a conversion lookup between a telephone number and an IP address. This service essentially centralizes the dial plan (all the telephone numbers in the network and how to reach them) in a single place in the network, as opposed to each node needing the configuration information to do this. This significantly eases the management of a large network.

Gatekeepers also provide other services, depending on the type of gatekeeper used. These services are discussed in this section:

- Telephone Address Lookup, page 6-11
- Call Admission Control, page 6-11
- Billing, page 6-12
- Using a Gatekeeper as a Proxy for Additional Services, page 6-12

Figure 6-5 shows a sample gatekeeper network.

Figure 6-5 Multinode Cisco Unified CME Gatekeeper Network



The following example shows the relevant dial peer configurations of the nodes shown in the network:

Note Note the use of **session target ras**; it is explained in the next section.

- Cisco Unified CME 1

```
dial-peer voice 2345 voip
   destination-pattern [2345]0..
   session target ras
   no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1345 voip
   destination-pattern [1345]0..
   session target ras
   no vad
```

- Cisco Unified CME 3:

```
dial-peer voice 1234 voip
   destination-pattern [1234]0..
   session target ras
   no vad
```

The following example shows a more detailed example from an individual Cisco Unified CME router setup to interwork with an H.323 gatekeeper connected via the Cisco Unified CME router's Ethernet interface. Note that the **gk ipaddr** comand defines the gatekeeper's IP address.

```
interface FastEthernet0/0
ip address 10.1.1.1 255.255.0.0
load-interval 30
duplex auto
speed auto
no cdp enable
h323-gateway voip interface
h323-gateway voip id gk ipaddr 10.1.10.1 1719
h323-gateway voip h323-id cme1
```

```
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 10.1.1.1

dial-peer voice 1234 voip
       destination-pattern [1-4]0..
       session target ras
       no vad
```

Telephone Address Lookup

The simplest type of gatekeeper provides only telephone number-to-IP address resolution. When a Cisco Unified CME system uses a gatekeeper to help route a call, it sends a message to the gatekeeper to request the IP address that corresponds to a certain specific phone number. As soon as Cisco Unified CME gets the correct IP address, it can send an H.323 call setup message for the desired phone number to the IP address of the remote Cisco Unified CME system (provided by the gatekeeper) that hosts that phone number. Instead of having a VoIP dial peer that points to every Cisco Unified CME system in your network, the Cisco Unified CME has only one dial peer that points to the IP address of the H.323 gatekeeper.

To reference a gatekeeper from a VoIP dial peer, use **ras** as the target instead of a specific IP address:

session target ras

In most cases, the H.323 gatekeeper gets the appropriate phone number-to-IP address configuration dynamically from the component Cisco Unified CME systems. For each individual phone number that is configured on a Cisco Unified CME system, the Cisco Unified CME system can send a Registration message to the gatekeeper. The Registration message basically says, "I'm an H.323 gateway-like device at IP address x.x.x.x, and I have phone number Y." The gatekeeper aggregates the information from the H.323 Registration messages from all the Cisco Unified CME gateways (and other H.323 gateways) into a composite database that contains all the current locations of all the telephone numbers in the network.

Call Admission Control

In addition to providing simple telephone number-to-IP address resolution, a gatekeeper can provide call admission control (CAC) for your VoIP network. CAC keeps track of the number of simultaneous VoIP calls present at each H.323 gateway and prevents overloading of the gateway's WAN links (and sometimes also provides load balancing for PSTN access ports). Without CAC, if too many calls attempt to use the same WAN link at the same time, either calls will fail in uncontrolled ways, or too many voice packets will try to get sent at the same time, leading to voice quality problems.

The Cisco Unified CME can do a limited amount of CAC itself without a gatekeeper, either by limiting the number of simultaneous calls associated with each dial peer or by using an end-to-end bandwidth reservation protocol called Resource Reservation Protocol (RSVP). However, per-dial peer call counting does not work well if you are using more than one dial peer per WAN link, and the RSVP mechanism requires end-to-end support of the RSVP protocol within your network infrastructure, so the gatekeeper-based CAC approach generally is far superior.

You can accomplish CAC with the following two Cisco IOS commands:

- **call threshold command**

  Using the **call threshold** command allows you to limit the number of calls allowed through a particular interface. This can be done with a single Cisco Unified CME. The following is an example:

  ```
  call threshold interface GigabitEthernet0/1 int-calls low 5 high 5
  ```

- **dial-peer command**

  Using the **dial-peer** command limits number of calls based on the **max-conn** parameter under the **dial-peer** command. This constraint to the specified maximum number of calls from given dial peer. A caveat associated with this command is that there are usually multiple dial peers on specific Cisco Unified CME and the Cisco Unified CME does not track the number calls across all dial peers. If a Cisco Unified CME does have multiple dial peers, with outbound and inbound calls, the dial-peer command solution will not work. If all inbound and outbound calls are routed through a single dial peer, this command is an effective option. The following is an example of the applicable **dial-peer** command:

```
dial-peer voice 10 voip
 max-conn 10
 destination-pattern 9T
 session target ras
 dtmf-relay h245-alphanumeric
 no vad
```

Billing

The gatekeeper keeps track of the number of active calls based on messages from the gateway indicating when individual calls start and stop. Because the gatekeeper knows the start and stop times and the called and calling phone numbers, a gatekeeper can provide a centralized point to connect to a billing service (for the VoIP calls).

This type of billing typically does not know about calls being made by a Cisco Unified CME system using its local PSTN connection. These calls do not involve H.323 VoIP call legs, so the H.323 gatekeeper typically does not see them. You can use the Cisco IOS Voice Gateway Remote Authentication Dial-In User Service (RADIUS) feature in conjunction with a central RADIUS server to track all Cisco Unified CME calls for both H.323 and PSTN for billing purposes.

Note Note that *syslog* is a viable option for accumulating call detail records (CDR) as an alternative to RADIUS as billing server. One limitation for syslog is that you cannot record billing account codes. All syslog messages (including system alerts/events that are not related to CDR) are sent to the syslog server. As a result, you will require a third-party application to parse relevant CDR info. However, to make CDRs viewable for operational purposes you will need a third-party application, even with RADIUS.

Using a Gatekeeper as a Proxy for Additional Services

The other major type of gatekeeper to consider is a *routed signaling gatekeeper*. Instead of simply providing phone number-to-IP address resolution, the routed signaling gatekeeper acts as an H.323 proxy device and participates in all the H.323 call signaling. With this type of gatekeeper, the Cisco Unified CME system sends the H.323 call setup directly to the gatekeeper. The gatekeeper then relays the H.323 setup to the final (or next-hop) destination. This is very similar to the Tandem Gateway hub-and-spoke VoIP call routing described earlier with Cisco Unified CME systems.

The routed signaling gatekeeper approach has two disadvantages:

- You tend to need more Routed Signal Gatekeepers because each individual gatekeeper has more work to do per call. Instead of just being primarily involved in the phone number-to-IP address resolution at the start of the call, a routed signaling gatekeeper stays involved throughout the call. It has to process all the H.323-related messages that pass through it.

- Routed signaling gatekeepers tend not to be transparent to the supplementary service ITU-T H.450 messages used for call transfer and forwarding between Cisco Unified CME systems. The presence of a routed signaling gatekeeper may actually prevent you from using H.450 services between Cisco Unified CME systems.

Note Certain extensions, such as MWI, call park, and intercom extensions should *never* register to the gatekeeper because these extensions have no meaning outside the local Cisco Unified CME system.

However, a routed signaling gatekeeper may be able to provide your network with additional services. This is generally truer in an H.323 VoIP network that is used for residential services. In this case, a routed signaling gatekeeper can provide services, such as call forwarding and call waiting, on behalf of H.323 endpoints that (unlike Cisco Unified CME) do not natively support these services. The situation can get more complicated in some service provider networks where the same VoIP infrastructure is used to provide both direct residential and hosted or managed enterprise and small or medium business VoIP services.

Finally, one other point that sometimes favors using routed signaling gatekeeper is in service provider networks, where there is a legal regulatory requirement to support lawful interception of telephone calls for government law enforcement agencies. In the United States this requirement is called Communications Assistance to Law Enforcement Agencies (CALEA). In this case, having the routed signaling gatekeeper present in both the signaling and media path for all calls to the H.323 endpoint allows wiretapping to take place such that it is undetectable to the H.323 endpoint that is having its voice calls monitored. If you are interested in building a private corporate VoIP network, however, you do not need to be concerned with this consideration.

Public and Internal Phone Numbers in an H.323 Network

You have already seen how a Cisco Unified CME system can register its phone numbers to a central H.323 gatekeeper to provide the VoIP network with a phone number-to-IP address directory. Now you must determine which phone numbers to register. In some cases, you may simply want to register all of them. The effect of this is to give all your Cisco Unified CME extensions a direct inward dial (DID) phone number that means that any extension within your Cisco Unified CME system can be called from anywhere in your VoIP network. However, when phone numbers are registered to a gatekeeper, they typically have to be in an appropriate form. In many cases, gatekeepers cannot handle raw (abbreviated) three- or four-digit extension numbers. Extension numbers typically must be converted into a format that looks more like regular PSTN phone numbers. For example, if you have extensions 1000 to 1099 on your Cisco Unified CME system, you may need to register them in long form as something like 408-555-0100 to 408-555-0199.

Registering secondary numbers for ephone-dn might be required if the DIDs you have been assigned are non-contiguous and do not fit into a particular pattern. For example, if you are assigned DID 408-555-0100 to 408-555-0125, and you want to map to internal extensions 1000 to 1025, you would use secondary dns:

```
ephone-dn 1
number 1000 secondary 4085550100 no-reg primary
!
ephone-dn 2
number 1001 secondary 4085550101 no-reg primary
!...and so on...
```

This makes the most sense when your Cisco Unified CME extension numbers also have matching real PSTN phone numbers. In this case, you probably have a PSTN link that uses an ISDN interface so that the PSTN network signals the calls from the PSTN number by providing you with the full national phone number of the number called. This type of numbering is often called E.164 format after the ITU-T recommendation that describes the transnational telephone number formatting rules. The term E.164 is often used a little loosely in that strictly using E.164 requires an indication of whether the phone number includes an international access code or otherwise.

One advantage of using E.164 numbers with a gatekeeper is that it simply gives you a larger number space to work with. This means that you are less likely to run out of phone numbers. It also makes it easier to add links to independent external VoIP networks if you need to. A larger number space also means that you can have overlapping extension numbers across different Cisco Unified CME systems. For example, you might have two Cisco Unified CME systems that (for historical reasons) need to use the same extension number range. You could have two Cisco Unified CME systems that both use the extension range 0100 to 0199, but have different E.164 numbers, such as 408-555-0100 and 510-555-0100. Using the full E.164 number helps resolve any potential conflict.

Cisco Unified CME can automatically convert your local extension numbers from two to five digits into E.164 format using the dialplan-pattern command. The following is a basic example:

```
telephony-service
       dialplan-pattern 1 40855501.. extension-length 4
```

The **dialplan-pattern** command causes the Cisco Unified CME system to attempt to match the extension numbers created by the **ephone-dn** command entries against the defined pattern. Using this example, the extension number 0123 would be matched against the final four digits of the dialplan pattern **01**.., where the **.** characters provide a wildcard match. The extension number 0123 would be expanded to 4085550123, and this number would be registered with the gatekeeper. You can define up to five different dialplan patterns. The 1 immediately following the **dialplan-pattern** command is simply a tag number, 1 to 5, that indicates which of the five **dialplan pattern** entries you are using.

The dialplan-pattern command can also perform leading-digit replacement for cases in which the extension number to E.164 number expansion is not a simple concatenation of a PSTN area code and prefix. The following example shows a more complex configuration.

```
telephony-service
    dialplan-pattern 1 5105yy99.. extension-length 3 extension-pattern 1..
```

Note The variable letter *y* in the preceding example represents arbitrary digits in the prefix of a telephone number. This convention is used when phone numbers outside the range of 555-0100 to 555-0199 are required for a given example.

Using the preceding example, extension 123 is expanded to E.164 number 5105yy9923. The three-digit extension number is matched first against the extension pattern and then is substituted into the E.164 pattern defined. Without this capability, simple truncation of the ten-digit E.164 number to a three-digit extension would result in three-digit extensions in the range 900 to 999, which causes a number plan conflict with the traditional “Dial 9 for an outside line.”

The **dialplan-pattern** command allows the Cisco Unified CME IP phone extension lines to be dialed using both the abbreviated two-to-five-digit extension number and the full E.164 or national phone number. In addition to helping with matching the called number on incoming calls, the **dialplan-pattern** command also promotes the *calling party* number included on outgoing calls from the extension to E.164 format. This is often a requirement on PSTN links using ISDN that usually will not accept abbreviated extension numbers as legitimate calling party identification. You have to choose your extension number range such that it does not conflict with the E.164 area code. For example, if your E.164 phone number is 408555xxxx, you cannot use extension numbers of the form 408x.

Note Using the **dialplan-pattern** command does not require you to use an H.323 gatekeeper.

You can turn off the gatekeeper registration triggered by the **dialplan-pattern** command using the **no-reg** command option at the end of the command.

Registering Individual Telephone Numbers with a Gatekeeper

If you do not want to register all your Cisco Unified CME system's extension numbers with a gatekeeper, you can omit usage of the global **dialplan-pattern** command, and control registration of each individual extension number from within the **ephone-dn** command that is used to create the extensions (or virtual voice ports).

Each ephone-dn allows you to assign a primary and secondary number to associate with the extension. You then have a choice to register both, either, or neither of these with the gatekeeper using the **no-reg**, **no-reg primary**, or **no-reg both** command options for the **ephone-dn number** command.

If you decide not to use the **dialplan-pattern** command, you can still provide the three-to-five-digit abbreviated number and full E.164 numbering for each ephone-dn by using the **secondary** number option, as shown in the following example.

```
ephone-dn 1
       number 0123 secondary 4085550123 no-reg primary
```

Using the secondary number allows incoming calls to the ephone-dn to use either 0123 or 4085550123 as the called number. It also only registers the secondary number 4085550123 to the Cisco Unified CME system's gatekeeper. This approach gives you control over what is registered on a per-ephone-dn basis.

Note that this approach does not modify the default calling party number selected on outgoing calls from the extension. In the preceding configuration example, the calling party number for outgoing calls is set to 0123. This is normally just fine for internal extension-to-extension calling. If you need to promote the calling party number to E.164 format for the benefit of VoIP or ISDN calls, you can do this using an IOS voice gateway translation rule applied to the call's outgoing dial peer.

You can mix and match the two approaches for controlling gatekeeper registration by using narrower extension pattern matches within the **dialplan-pattern** command. For example, instead of using **extension-pattern 10.**. to match all the extensions in the 0100 to 0199 range, you can add multiple (up to five) **dialplan-pattern** commands that have narrow match ranges such as **extension-pattern 012.**, which matches only extension numbers in the 0120 to 0129 range.

If you do not have enough E.164 DID numbers available, but you still need a few extra extension lines, you can assign them to a different range of numbers. You can then use the **dialplan-pattern** command to register E.164 phone numbers in the match range with a gatekeeper. For example, you might give all your employees extension numbers in the 0100 to 0199 range, have these match a **dialplan-pattern** and, thus, register to a gatekeeper, and then simply assign nonemployee phone numbers, such as break room and lobby phones, into a separate range that does not have corresponding DID E.164 numbers, as shown in the following example.

```
telephony-service
       dialplan-pattern 1 40855501.. extension-length 4
ephone-dn 1
       number 0123
       name employee1
ephone-dn 2
       number 0124
       name empolyee2
ephone-dn 3
```

```
number 2001
name BreakRoom
```

In the preceding configuration example, the extension numbers 0123 and 0124 are registered with the gatekeeper as 4085550123 and 4085550124. The break room extension 2001 is not registered.

With this approach, one final detail to take care of is deciding what calling party number identification you want to provide for ISDN or VoIP calls placed from the break room phone. The simplest solution is to add a translation rule on the outgoing dial peer for calls from the break room phone to map the calling party number to your main or receptionist E.164 number, such as 4085550100. You may choose to do this for all outgoing calls from all extensions if you do not want the called party to be able to see individual extension numbers.

Internal and External Callers for VoIP

With the **dialplan-pattern** command, you can cause certain incoming VoIP calls to be treated as "internal" calls. By default, calls between IP phones on the same Cisco Unified CME system are treated as internal calls and ring with an internal ringer cadence. All other calls (VoIP and PSTN) are treated as external calls and ring with a different external call ringer cadence. Analog phones attached to router Foreign Exchange Station (FXS) voice ports also are treated as external calls by default. However, incoming calls that have calling party numbers that match one of the available five **dialplan-pattern** commands are treated as internal calls.

For example, suppose you have two Cisco Unified CME systems linked via VoIP and you use extension numbers 100 to 299 with E.164 numbers 4085yy0100 to 4085yy0199 on one system and extension numbers 200 to 299 with E.164 numbers 5105yy0200 to 5105yy00299 on the second system. You can create **dialplan-pattern** commands on both systems that provide extension number matches for both systems, as shown in the following example.

```
telephony-service
      dialplan-pattern 1 4085yy01.. extension-length 3
      dialplan-pattern 2 5105yy02.. extension-length 3
```

Note The variable letter *y* in the preceding example represents arbitrary digits in the prefix of a telephone number. This convention is used when phone numbers outside the range of 555-0100 to 555-0199 are required for a given example.

Any incoming calls that match either of the dialplan patterns are treated as internal calls, regardless of where the call physically originates. When the incoming calling party number matches the dialplan pattern, the Caller ID displayed for the call is demoted from E.164 format back to abbreviated three-to-five-digit extension number format. Also, the call is presented using the internal ring cadence. This allows you to treat incoming VoIP calls from other Cisco Unified CME systems within your network as internal calls.

To make a call coming from a router FXS voice port appear as an internal call, you need to set the voice port **station-id number** to match the dialplan pattern number range, as shown in the following example.

```
voice-port 1/0/0
       station-id number 4085550188
       station-id name AnalogPhone
dial-peer voice 408188 pots
       destination-pattern 4085550188
       port 1/0/0
       no vad
dial-peer voice number 188 pots
       destination-pattern 188
       port 1/0/0
       no vad
```

This configuration causes calls from the analog phone to have caller ID 4085550188. It also allows the analog phone to be called by dialing either the long form 4085550188 or the abbreviated three-digit extension number 188.

Note Calls from analog phones that are attached to Cisco Analog Telephony Adapters (Cisco ATAs) are treated as IP phones and do not need any special treatment.

DTMF Relay for H.323

Dual-tone multifrequency (DTMF) relay is a mechanism for reliably carrying DTMF digits across VoIP connections. If you need to signal the 0 to 9, *, and # keypad digits (DTMF digits) from your IP phone across your VoIP network, you must configure DTMF relay. DTMF digits are also sometimes called TouchTone digits.

You should configure DTMF relay if you want to operate a remotely connected voice mail system, use calling card access for PSTN calls placed through a remote VoIP PSTN gateway, or access any type of DTMF-driven interactive voice response (IVR) system (for example, telephone banking or airline flight information services).

The following sections discuss DTMF deployment considerations in the context of Cisco Unified CME networks:

- DTMF Digits, page 6-17
- Transporting DTMF Digits Reliably Using DTMF Relay, page 6-18
- Different Forms of DTMF Relay, page 6-18

DTMF Digits

DTMF describes a method of encoding telephone digits using two audio tones. For a conventional telephone keypad in which the keys are arranged in three columns by four rows, the first audio tone selects the row of the key, and the second audio tone selects the column. Each row-and-column tone uses a different audio frequency (pitch). This method of telephone digit signaling replaced the old-fashioned loop disconnect (dial pulse) digit dialing used by old rotary-style analog phones.

There are 16 DTMF digits (arranged as four columns by four rows). In addition to the standard 12 keypad digits—0 to 9, *, and #—an additional four digits form an extra fourth column of digits called simply A, B, C, and D. Because the ABCD digits are unavailable on a normal phone keypad, you are unlikely to

ever come across these for normal phone calls. They are used occasionally by voice mail systems to operate an intersystem exchange of voice messages between separate voice mail systems using a standard called Analog Message Interchange Standard (AMIS).

Some security-type phones also use the ABCD digits for initial negotiation. You may also see these used in some Cisco Unified CME configuration examples where there is a need to create telephone numbers that cannot be directly dialed from a phone keypad. One example of this is if you want to create nondialable phone numbers for intercoms. You normally place an intercom call by pressing a button specifically configured for intercom (this works somewhat like a speed-dial button), so you do not need to be able to enter individual dialed digits.

Transporting DTMF Digits Reliably Using DTMF Relay

In the simple case of analog phones, the phone keypad digits result in the generation of DTMF audio tones. DTMF signaling works fine for analog phones connected directly to PSTN analog subscriber lines that travel only a relatively short distance to reach a central office (CO) telephone exchange. However, when the analog phone is connected to a VoIP system, and telephone calls are made using compressed voice (for example, G.729 at 8 Kbps), there is a substantial risk that the audio tones of the DTMF digits sent through the compressed voice path may become too distorted to be predictably recognized correctly by a remote voice mail system.

Even when you use uncompressed G.711 A-law/μ-law 64 Kbps for VoIP calls, there is still a risk that DTMF digits can get distorted in transit. This is because of the risk of packet loss in the VoIP network. If the network drops an occasional IP packet containing voice, this is usually imperceptible to the human ear. However, if an IP packet is dropped that contains an audio encoding of part of a DTMF tone, this is probably to keep the DTMF digit detection in the far-end system from detecting the digit (or to make it erroneously detect multiple digits). This is also the reason that other nonvoice audio signals such as fax and data modems need special treatment in VoIP networks.

To work around this issue, you generally have to use some form of DTMF relay. DTMF relay causes the digit press to be detected by the PSTN trunk or analog phone interface on the VoIP gateway. The originating VoIP gateway then signals the digit as an explicit event to the far-end VoIP gateway and removes the audio signal for the DTMF from the voice packet stream. When the far-end VoIP gateway receives the signal for the DTMF event, it regenerates the DTMF audio signal and inserts it into the outgoing audio stream to the PSTN or analog phone.

In the case of the Cisco SCCP IP phones, the digit never exists as an audio signal from the VoIP perspective, because it is directly signaled via SCCP. The digit audio that the phone user hears from the phone handset is for the benefit of the phone user only and is not passed to the VoIP connection.

Different Forms of DTMF Relay

In general, there are two main ways to signal DTMF events between VoIP gateways: H.245 digit relay and Real-Time Transport Protocol (RTP)-based DTMF digit relay. This is true for both H.323 and SIP, although the specific details are different.

The H.245 digit relay option sends a message via the H.323 control channel that is associated with the VoIP call. (This is called H.245 digit relay because it uses the H.245 control channel part of the H.323 protocol to signal the digit event.)

The RTP-based DTMF digit relay method carries the digit event through the voice media channel as a special marked RTP media packet. The problem of possible IP packet drop is overcome by sending multiple redundant copies of the event so that even if one of the copies is lost, there is little chance that all copies will be lost.

H.245 Digit Relay

There are two types of H.245 digit relay: signal and alphanumeric. The dial peer commands for these are **dtmf-relay h245-signal** and **dtmf-relay h245-alphanumeric**.

In signal mode, two events are sent: one to indicate the start of the digit and one to indicate the end of the digit. This lets the duration of the keypress on the phone be reflected in the duration of the digit regenerated by the far-end VoIP gateway. This is useful for calling card PSTN access where a long-duration press of the # key is sometimes used to indicate the end of a calling card call plus the intention to place a follow-on call (without needing to reenter a calling card number and its associated PIN).

Alphanumeric mode has only a single event signal. This results in the regeneration of a fixed-duration DTMF signal (usually 200 milliseconds) by the far-end VoIP gateway. In this mode, the length of the regenerated digit is unrelated to how long you press the keypad button on the phone. Some implementations generate the alphanumeric DTMF signal when you press the phone's keypad button, and others generate the signal when you release the keypad button. You can use this duration-of-press-independent property to tell which type of VoIP DTMF digit relay is being used.

H.245 alphanumeric mode is the one that should be used with Cisco Unified CME IP phones.

RTP Digit Relay

RTP-based digit relay mode also has two types:

- **RFC 2833**—A standards-based mechanism, sometimes called *Named Telephony Events* (*NTE*) or *Named Signaling Events* (*NSE*). The Cisco IOS **dial peer** command for this mode is **dtmf-relay rtp-nte**. This method is prevalent in SIP VoIP networks.
- **cisco-rtp**—A Cisco proprietary mechanism that represents an implementation of RTP-based DTMF relay that predates the RFC 2833 standard. The dial peer command for this is **dtmf-relay cisco-rtp**. If you enable the **dtmf-relay** command without specifying an explicit DTMF relay type, you get the cisco-rtp type.

When you press a keypad digit on an IP phone, you hear a tone in the phone handset that corresponds to the digit you press. Although you hear this audio tone, the far-end party that your call is connected to does not. The IP phone sends the keypad audio signal only to the phone's handset (or speaker). It does not insert the audio digit indication into the outgoing voice packet stream. When you press the keypad digit on an SCCP-based IP phone, the phone sends a control message to the Cisco Unified CME router via SCCP. Because the digit press originates from the phone as a control channel message, the SCCP digit message is simply converted into an H.245 alphanumeric message to send this across H.323 VoIP.

The SCCP digit press event does not indicate the duration of the keypad button press. This means that the H.245 signal method cannot be used, because the SCCP phone does not provide digit-start and digit-stop information. Also, the SCCP phones do not natively support either the RFC 2833 or cisco-rtp RTP-based digit relay mechanisms.

For you to signal DTMF keypad digits across H.323, you need to configure your VoIP dial peers as shown in the following example:

```
dial-peer voice 510200 voip
       destination-pattern 51055502..
       session target ipv4:10.1.1.1
       dtmf-relay h245-alphanumeric
       no vad
```

If you are using your Cisco Unified CME system in a SIP network, you have to use the RFC 2833 DTMF relay method where possible. Cisco Unified CME 3.2 (and later) software provides automatic conversion from the SCCP control channel DTMF messages received from the SCCP IP phone into standard SIP RFC 2833 RTP digits.

Call Transfer and Call Forwarding in an H.323 Network Using H.450 Services

The ITU-T H.450 services are a set of standard supplementary services defined for H.323 VoIP networks. H.450 provides services above and beyond basic A to B telephone calls.
Cisco Unified CME 3.0 offers only the services related to call transfer (H.450.2) and call forwarding (H.450.3). Cisco Unified CME 3.1 also introduced support for the H.450.12 capabilities discovery protocol to ease interworking issues with another company's H.323 systems.

The following is a full list of the H.450.x services, including the date when they became formal ratified ITU-T standards:

- **H.450.1 (2/1998)**—A generic functional protocol that supports supplementary services in H.323 (supported by Cisco Unified CME)
- **H.450.2 (2/1998)**—A call transfer supplementary service for H.323
- **H.450.3 (2/1998)**—A call diversion supplementary service for H.323 (supported by Cisco Unified CME)
- **H.450.4 (5/1999)**—A call hold supplementary service for H.323
- **H.450.5 (5/1999)**—A call park and call pickup supplementary service for H.323
- **H.450.6 (5/1999)**—A call waiting supplementary service for H.323
- **H.450.7 (5/1999)**—An MWI supplementary service for H.323
- **H.450.8 (2/2000)**—A name identification service
- **H.450.9 (11/2000)**—A call completion supplementary service for H.323 (includes callback for a busy subscriber)
- **H.450.10 (3/2001)**—A call offering supplementary service for H.323 (includes camp-on busy subscriber)
- **H.450.11 (3/2001)**—A call intrusion supplementary service for H.323
- **H.450.12 (7/2001)**—A common information additional network feature for H.323 (for H.450.x capabilities discovery, supported by Cisco Unified CME 3.1 and later releases)

An important thing to note about the dates these standards became available is that many H.323 networks were brought into service before these standards were issued. This means that support of these standards within H.323 networks varies widely, which causes some challenges in deploying these services within multivendor H.323 networks.

H.450.2 and H.450.3 services are present and enabled by default in Cisco IOS Release 12.3(4)T and later releases (for voice-enabled images). This allows a Cisco IOS voice gateway (without Cisco Unified CME configuration) to be used as a VoIP-to-PSTN gateway and to automatically support the forwarded party, transferee, and transfer-to roles when using the standard default voice session application.

The earlier Cisco IOS Release 12.2(15)T and later releases can also support H.450.2 and H.450.3 provided that they are configured to use a special Tool Command Language (TcL) script (called app_h450_transfer.tcl and available on Cisco.com) in place of the default voice session application.

H.450.12 services are available in Cisco IOS Release 12.3(7)T. They need to be explicitly enabled using the **supplementary-service** command.

The following sections address issues related to call transfer and call forwarding in an H.323 network using H.450 services:

H.450.2 Call Transfer

For call transfer with consultation, the basic operation of the telephone user interface is expected to look like this:

1. The inbound call to the phone is answered. The parties talk.
2. The phone user (transferor) presses the transfer key, gets dial tone, and enters the transfer-to destination. The calling party (transferee) is placed on hold and may hear the music on hold audio feed.
3. The transferor hears the transfer-to phone start to ring.
4. The phone at the transfer-to destination is answered, and a consultation call takes place between the transfer-to and the transferor.
5. The transferor presses the transfer key a second time (or simply hangs up) to execute the transfer.
6. The original caller (the transferee) is connected to the transfer-to party.

The H.450.2 protocol is designed to allow this operation to take place where the transferee, transferor, and transfer-to parties are all associated with different H.323 endpoints, regardless of physical location. This means (for example) that a transferee party originating a call in Paris can place a call to a transferor in Los Angeles and get transferred to a transfer-to destination in London. In a VoIP network that fully supports H.450.2, the resulting post-transfer call between Paris and London is a direct call and does not have to be relayed via the transferor (in Los Angeles). This is an especially important consideration when you consider the network design implications from a voice quality, delay, and scalability point of view. It is an important consideration for cases in which a call might need to be transferred multiple times before it reaches its final destination.

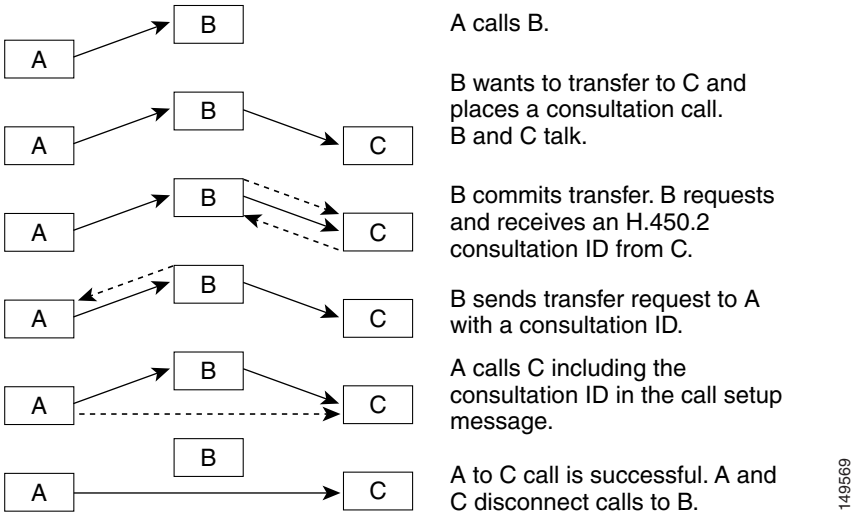
Multiple transfer is one area in which VoIP-based networks have considerable superiority over traditional legacy-based TDM networks—if they are implemented to take full advantage of the H.450.2 service.

There are other ways of invoking a call transfer that do not follow the usual user interface steps. One particular example is a three-party conference call where A calls B, B calls C, and then B joins the A–B and B–C calls together as a conference. If the B party conference initiator wants to drop out of the conference and leave the A and C parties connected to each other, this can be implemented as a call transfer where B invokes a transfer of A to C.

The following detailed protocol transactions allow the transfer to take place (see Figure 6-6):

1. The original incoming call is just an ordinary "A calls B" H.323 call between two parties. Of course, the original call does not have to be an incoming call. For example, it could be an outgoing call placed by an assistant on behalf of an executive who is transferred to the executive as soon as the call is successfully connected.
2. The transferring party presses the transfer key. This puts the original call on hold. A second line or call instance is acquired on the transferor's phone, and dial tone is obtained. The transferor dials the phone number of the transfer-to destination using the second line or call instance. This consultation call is also a simple "B calls C" H.323 call between two parties. To the external H.323 network, the A–B and B–C calls are seen as unrelated at this point. At this stage in the process, there is no guarantee that a transfer will actually take place. The B–C call can return a busy indication, and the B (transferor) party can elect to try a different transfer-to destination, D. The B–C call may connect, and a consultation call may take place in which C declines to talk to A. The B–C call can terminate at that point, and the transferor B party may then resume the A–B call. Alternatively, B can place another consultation call B–D.
3. The transferor B decides to commit the transfer either by pressing the transfer button a second time or by hanging up. At this point, a complex sequence of actions takes place in an attempt to transfer the call. First, the transferor B puts the B–C call into a hold state and then sends an H.450.2 message to the transfer-to destination C. This informs C that a transfer will take place and requests that C issue a unique consultation ID to B. This consultation ID is used to identify the call that is being transferred.
4. When B receives the consultation ID from C, it sends an H.450.2 transfer request to A containing the consultation ID. This message includes the phone number for C.
5. When the A party (the transferee) receives the transfer request, it places a direct H.323 call to C using the phone number provided by B. This call includes the consultation ID that was generated by C and passed via B (the transferor). The transfer-to destination receives the A–C call from A. At this point the B–C consultation call is still active. The transfer-to C destination uses the consultation ID from the A–C call to match the B–C call. Because the B–C and A–C calls have the same consultation ID, the transfer-to C party can tell that the A–C call is intended to replace the B–C call.
6. As soon as the transfer-to C has matched up the A–C and B–C calls using the consultation ID, C disconnects the B–C call. When the transferee A gets a successful call response from C so that the A–C call enters the connected state, the transferee A disconnects the A–B call. The transferor B party gets a disconnect indication for both the A–B and B–C calls and drops out of the transferred call.

Figure 6-6 H.450.2 Call Transfer Protocol



A couple of minor variations on this flow are worth mentioning. The transferor phone user at B can choose to commit the transfer before the B–C consultation call is answered, while the B–C call is still in the alerting (ringing) state. The B to C consultation ID request can take place regardless of whether the B–C consultation call is in the connected or alerting (ringing) state.

The transferor phone B can be configured to invoke a transfer to C without first placing a consultation call. In this case, the B to A call transfer request carries a zero consultation ID. This type of transfer has the disadvantage that B has no guarantee that the A–C transferred call will succeed. It has the advantage that it does not require the transfer-to C destination to support the H.450.2 protocol and the associated B–C-to-A–C call replacement operation. This type of blind transfer is useful when the transfer-to destination is some type of automatic voice system, such as a voice mail device or a call queuing service.

So, as you can see, you can invoke three types of transfers using the H.450.2 call transfer protocol:

- Transfer with consultation with the transfer committed when the B–C call is in the connected state. Cisco Unified CME calls this type *full consult with transfer at connected*.
- Transfer with consultation with the transfer committed when the B–C call is in the alerting (ringing) state. Cisco Unified CME calls this type *full consult with transfer at alerting*.
- A blind transfer that does not involve a consultation call. Cisco Unified CME calls this type a full-blind transfer.

Cisco Unified CME lets you mix and match the full-consult and full-blind transfer types at several levels:

- Configure a global default using the **transfer-system** command (under **telephony-service**) and select either **transfer-system full-consult** or **transfer-system** full-blind.
- Override the global transfer system selection for each IP phone line (ephone-dn) using the **transfer-mode** command. You can select either **transfer-mode consult** or **transfer-mode blind**. For example, you might choose to have a receptionist phone that deals with a high volume of calls always perform blind transfers.
- Use the **transfer-pattern** command to force selection of the blind transfer mode for specific transfer-to destination numbers. The t**ransfer-pattern** command is also used to set up transfer permissions for nonlocal transfer-to destinations. This is useful if you need to prohibit trunk-to-trunk transfers and prevent toll fraud.

Now that you understand the process for H.450.2 call transfer, the next section discusses H.450.3 call forwarding.

H.450.3 Call Forwarding

For call forwarding, as with call transfer, the following apply:

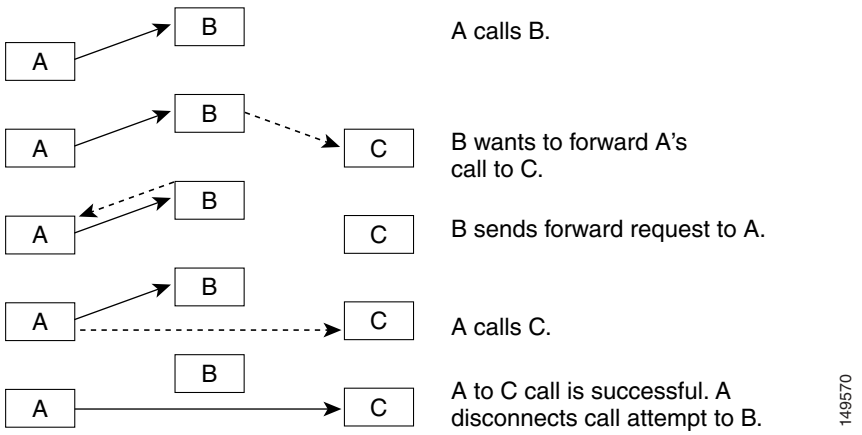
1. An inbound call is placed to an IP phone.
2. The IP phone is busy, does not answer, or is configured for unconditional call forwarding (call forward all).
3. The IP phone forwards the call to an alternate destination.
4. The original calling phone may optionally receive a display update to show that the call has been forwarded. This can be an important issue if billing or cost differences depend on the location of the final destination.
5. The IP phone at the alternate destination answers the call or may forward it to another destination. The IP phone that receives the forwarded call receives information that lets it know that the call was forwarded. This may include information about the original called number.

The H.450.3 protocol is designed to allow this operation to take place where the original calling party, forwarding phone, and forward-to party are all associated with different H.323 endpoints, regardless of physical location.

This means, for example, that a calling party originating a call in Paris can place a call to an IP phone in Los Angeles and get forwarded to a destination in London. In a VoIP network that fully supports H.450.3, the resulting forwarded call between Paris and London is a direct call and does not have to be relayed via the forwarder (in Los Angeles).

The H.450.3 forwarding protocol details are quite a bit simpler than the H.450.2 transfer case. When call forwarding takes place on an A to B call, the forwarding party B simply sends an H.450.3 message back to the calling A party to request that A call C (the forward-to destination). Generally, there is no requirement that the C party be aware of the H.450.3 protocol message exchange between A and B. If the A party accepts the call forwarding request, the A party disconnects the original A–B call, as shown in Figure 6-7.

Figure 6-7 H.450.3 Call Forwarding Protocol



You activate the H.450.3 service using the **call-forward pattern command**. This is designed to let you selectively invoke the end-to-end H.450.3 style of call forwarding based on matching the calling party phone number. To invoke H.450.3 for all possible calling party numbers, you configure **call-forward pattern .T**, where the **.T** pattern parameter provides a wildcard match of any length.

Note because all calling party numbers are not known, in an H.450 network you should always enable the **call-forward pattern .T** command.

If you do not configure the H.450.3 service, by default you are restricted to forwarding incoming VoIP calls only within the scope of the local Cisco Unified CME system. The local scope includes forwarding to other local IP phones or to voice ports physically connected to the router (including PSTN access).

Caution If you permit call forwarding of incoming PSTN calls into outgoing PSTN calls where your PSTN interface uses simple analog Foreign Exchange Office (FXO) ports, you may have a problem with disconnect supervision. In many cases, your PSTN provider will not have enabled call disconnect signaling on the PSTN subscriber lines connected to your FXO ports. For the case of a PSTN FXO-to-FXO hairpin call path, this can result in hung voice ports, because there is no signaling of disconnect when the remote PSTN parties hang up. If you encounter this problem, you need to contact your PSTN service provider to enable disconnect supervision on your PSTN phone lines. Note that for most PSTN hairpin call paths, the caller ID of the original caller is replaced by the caller ID of the outgoing PSTN interface.

H.450.12 Supplementary Services Capabilities

The H.450.2 and H.450.3 protocols can give you a significant degree of flexibility in distributing and moving H.323 calls in your VoIP network regardless of geographic location considerations. At the same time, this can present a challenge when you attempt to deploy these services into an existing H.323-based network where support of H.450.x is not widespread.

To help you operate H.450.2 and H.450.3 services in a mixed-capability network, Cisco Unified CME 3.1 introduced support of H.450.12. The formal name for this service is *Common Information Additional Network Feature for H.323*. Basically, this means that H.450.12 provides an H.450.x service capabilities exchange between H.323 endpoints.

The H.450.12 protocol allows Cisco Unified CME to detect the H.450.x service capabilities that are available on a call-by-call basis. This allows the Cisco Unified CME system to safely invoke H.450.2 transfer and H.450.3 forwarding without risk of dropping calls, because one or more of the remote endpoints involved in the call does not support H.450.

If Cisco Unified CME detects that H.450.2 or H.450.3 is not supported for the call, you can configure Cisco Unified CME to support the transfer or forwarding by locally bridging together the call legs to form VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call paths. The term *hairpin* is used because the call path doubles back on itself in a U shape that resembles a hairpin. You may sometimes see this type of call path called *tromboning*, because a trombone has a similar U shape.

In the case of a call transfer, this means that the A–B original call and the B C consultation calls are retained and then simply bridged together to create a hairpin or Cisco IP-to-IP Gateway call A-to-B-to-C. In the case of a call forward, the call path for A calls B and B forwards to C also becomes A-to-B-to-C.

The Cisco Unified CME 3.1 code has the restriction that to successfully hairpin or Cisco IP-to-IP Gateway VoIP calls, the call legs for the A–B and B–C segments must have compatible properties. This primarily means that the A–B and A–C call legs must both use the same voice compression codec (either G.729 or G.711). This restriction does not apply in the special case that either A and B or B and C are phones or voice ports connected to the same Cisco Unified CME system.

Cisco Unified CME 3.2 allows you to overcome this single-codec restriction, because it supports SCCP-based digital signal processor (DSP) farms that can be used to provide transcoding of voice packets between the bridged call legs. The DSP farm transcoding service supports conversion of G.711 voice packets to G.729 as needed.

With the VoIP-to-VoIP Cisco IP-to-IP Gateway call routing approach, you lose the final call path optimization that you would get if H.450.x were fully supported. Costs associated with this nonoptimal call routing include extra bandwidth used and additional end-to-end delay in the voice path.

DSP Resources for Transcoding

DSP resources is a group of one or more DSPs that are not directly associated with any physical interfaces (such as PSTN voice ports). Instead, the DSPs are available as a pool of signal processing resources that can be used to provide additional processing services for telephony calls. The primary applications that require DSP resource services are transcoding for VoIP hairpin calls and transcoding for G.729 three-party conferencing. Support for DSP resources for transcoding is available in Cisco Unified CME 3.2 and later versions.

The term *transcoding* describes the operation of converting a telephone call that is encoded (compressed) using one type of voice coder-decoder (codec) into another. Specifically, transcoding is used to convert voice packets between the G.711 (64 Kbps) and G.729 (8 Kbps) compression formats.

Cisco Unified CME supports the use of DSP resources for only transcoding services. It does not support DSP resources for conferencing services, although it does use DSP resources to support three-party conferencing for G.729 VoIP calls. The Cisco Unified CME three-party conferencing service uses software-based audio mixing of G.711 audio streams. When Cisco Unified CME needs to conference three-party G.729 calls, it uses the DSP transcoding service to convert the G.729 audio into G.711 and then applies the G.711 software-based audio mixing to the transcoded G.711 audio. DSP resources require separate physical DSPs for the transcoding-versus-conferencing service. It is generally more cost-effective to support G.729 three-party conferencing via a transcode-plus-software-mixer approach rather than dedicating whole DSPs to support just the conferencing service.

Although the DSPs in a resource pool are not directly associated with physical voice ports, they are hardware devices. If you need DSP resource services, you have to consider how and where you can attach these to your Cisco Unified CME system.

The DSP resource systems that Cisco Unified CME supports are the same as those used by Cisco_Unified CallManager. So this is one more place where we provides investment protection in case you ever need to redeploy hardware originally purchased for Cisco Unified CME into Cisco Unified CallManager environments (or vice versa).

You can attach DSPs to Cisco Unified CME systems in a number of ways. The simplest way is to insert DSP modules into the DSP sockets on the motherboards of some of the newer routers, such as the Cisco 2800 and Cisco 3800 series Integrated Services Routers (ISRs).

For Cisco routers that do not have motherboard DSP sockets, you can usually overprovision extra DSPs into voice network modules (NM) such as the NM-HDV and NM-HDV2 that are used to provide PSTN interfaces. The extra DSPs in these modules that are not needed to support the PSTN interface connections can be configured as DSP resource pools.

The DSP resources do not even have to be in the same physical router as Cisco Unified CME. The DSP resources are operated and controlled using SCCP over TCP/IP. This means that you can use a spare NM slot in a second router (that supports DSP resources) and have it controlled by a Cisco Unified CME in a separate router. In practice, the Cisco Unified CME and DSP resource routers do need to be connected locally over Ethernet or some other high-bandwidth interface.

Because the DSP resources are operated using SCCP, this means that, just as with the SCCP IP phones, the SCCP DSP resources can be used in support of either H.323 or SIP networks.

The configuration steps for DSP resources are too detailed to include in this publication. However, they are covered in detail in the *Cisco Unified CME 3.2 System Administrator Guide*. Look for the **dspfarm** command for configuring the actual DSP resources and the **sdspfarm** command for configuring the Cisco Unified CME to manage the DSP resources.

Configuring H.450.x Services

This section provides a quick look at the Cisco IOS commands that you use to configure H.450 services. To enable basic H.450.2 and H.450.3 call transfer and call forwarding, you use the **transfer-system** and **call-forward pattern** commands, as shown in the following example.

```
telephony-service
       ip source-address 10.1.1.1 port 2000
       max-ephones 24
       max-dns 48
       transfer-system full-consult
       call-forward pattern .T
       create cnf-files
```

To turn on the H.450.12 service (in Cisco Unified CME 3.1 and later), use the following:

voice service voip

supplementary-service h450.12

To permit VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call routing to work with remote H.323 endpoints that do not support H.450.x service, use this:

voice-service-voip

allow-connections h323 to h323

Older Cisco Unified CME 3.0 and earlier code does not support the H.450.12 service. This means that if you enable H.450.12 on a Cisco Unified CME 3.1 system and place a call from a Cisco Unified CME 3.0 system, the Cisco Unified CME 3.1 system will incorrectly infer that H.450.x services are not supported by the Cisco Unified CME 3.0 system.

The workaround for this upgrade issue it to operate the H.450.12 service in advertise-only mode. In this mode, your Cisco Unified CME system transmits H.450.12 capability indications for the benefit of remote H.323 systems that are H.450.12-aware, but it does not require receipt of H.450.12 indications from a remote H.323 endpoint. You can then manually disable the H.450.2 and H.450.3 service for each non-H.450-capable VoIP link using per-dial peer configuration, as shown in the following example.

```
voice service voip
       supplementary-service h450.12 advertise-only
       allow-connections h323 to h323
dial-peer voice voip 5000
       destination-pattern 50..
       session target ipv4 10.1.20.1
       no supplementary-service h450.2
       no supplementary-service h450.3
       no vad
```

With this configuration, no attempt is made to invoke H.450.2 transfer and H.450.3 forwarding for calls using the VoIP dial peer. Instead, VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call routing is used.

Cisco Unified CME Local Supplementary Services

Cisco Unified CME is designed to make use of H.450.2 call transfer and H.450.3 call forwarding for all calls that involve one or more VoIP call legs. For example, for an incoming H.323 VoIP call that is internally forwarded from one local IP phone to a second IP phone, Cisco Unified CME sends an H.450.3 response back to the original calling party. This causes the caller to cancel the original H.323 call to the Cisco Unified CME system's first phone and creates a new H.323 call back to the Cisco Unified CME using the second phone's number.

At first, this might seem like doing things the hard way. However, the point of doing this is to make sure that the original caller can see that the call has been forwarded. Returning the call to the originator and to issue a new call allows the calling party system to have full visibility of what is going on and allows the display on the calling phone to be updated accordingly. This is an important feature if you are trying to create a seamless multisite Cisco Unified CME network as part of an internal enterprise-wide phone system.

You can use the **supplementary-service** commands to disable this VoIP end-to-end behavior and invoke hairpin and Cisco IP-to-IP Gateway call handling. For the special case in which the forwarding phone and forward-to phone are part of the same Cisco Unified CME system, the hairpin and Cisco IP-to-IP Gateway call routing mechanism can be used without incurring any real-world penalty. For incoming VoIP calls that are locally forwarded within a single Cisco Unified CME system, the final call and media path are the same, regardless of which mechanism you use to handle call forwarding. Although this example describes only local call forwarding, the same principle applies to call transfer.

Also, it is important to stress that the complexities associated with the H.450.x end-to-end services apply only to calls that involve at least one VoIP call leg. For simple standalone Cisco Unified CME usage, in which all external calls directly use the router's PSTN interfaces, Cisco Unified CME operation is more simplified. However, to use call transfer with consultation, you still need to configure **transfer-system full-consult**.

H.450.x and Cisco Unified CallManager

Cisco Unified CallManager (as of 4.0) does not support H.450.x services, including H.450.12. However, Cisco Unified CME 3.1 (and above) automatically detects a call that involves a Cisco Unified CallManager using special H.323 nonstandard information elements (IEs). Even without an H.450.12 indication, Cisco Unified CME system's automatic Cisco Unified CallManager detection can be used to invoke VoIP-to-VoIP hairpin or Cisco IP-to-IP Gateway call routing when needed for call transfer and forwarding. You need to enable the **allow-connections h323 to h323** command to make this work.

Some special configuration of the H.323 interface on Cisco Unified CallManager may also be required, depending on the specific Cisco Unified CallManager software version used. For example, you may be required to configure a Media Termination Point (MTP), disable H.323 Fast, Start, and use Cisco Unified CallManager system's H.323 Inter-Cluster Trunk (ICT) mode.

H.450.x Proxy Services

You have seen how you can use Cisco Unified CME to create VoIP-to-VoIP call paths for call forwarding and transfer initiated by IP phones attached to Cisco Unified CME. What may not be obvious is that this same mechanism can be applied to calls that simply need to pass physically through a router. This is true regardless of whether the router is configured as a Cisco Unified CME with IP phones attached. Calls that pass through a router as a result of deliberate H.323 call processing (within the router) are not the same as calls that pass through the router at the basic IP packet routing and IP connectivity level. The distinction being made here is the difference between routing H.323 calls and routing IP packets.

When a call passes through a router and the router is used in onward routing of the called number, this is called Cisco IP-to-IP Gateway. In the special case that the Cisco IP-to-IP Gateway call routing results in the call entering and exiting the router on the same VoIP interface, the result is a VoIP-to-VoIP hairpin call.

A Cisco Unified CME system that is deployed at a remote branch office typically has only a single WAN and VoIP interface. This means that all VoIP-to-VoIP call paths created by the Cisco Unified CME inevitably are of the hairpin form. Hairpin VoIP-to-VoIP paths are inherently undesirable, because the doubled-back voice path is an inefficient use of scarce WAN bandwidth.

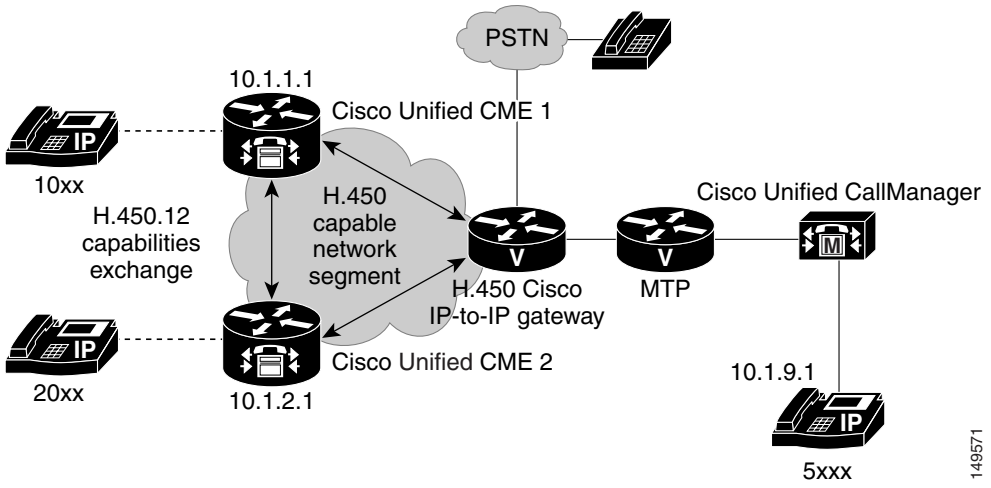
The more general VoIP-to-VoIP Cisco IP-to-IP Gateway case may offer some real advantages. One example is when you choose to use VoIP Cisco IP-to-IP Gateway call routing to provide a proxy for H.450 services.

Consider a VoIP network that connects to a central Cisco Unified CallManager system at a company's central site. Assume that the central site has a single voice mail system. Attached to the central system are a number of remote branches with Cisco Unified CME systems connected over WAN links in a hub-and-spoke arrangement, with the Cisco Unified CallManager site acting as the hub. Because the Cisco Unified CallManager does not support H.450 services, a call from the Cisco Unified CallManager site to a remote Cisco Unified CME system that is forwarded-on-busy to a voice mail system at the central site is VoIP-to-VoIP hairpin routed. This means that the call and media path for the voice mail call extends all the way from the central Cisco Unified CallManager to the remote Cisco Unified CME site and then hairpins back to the central voice mail. This consumes two calls worth of bandwidth on the WAN link and could potentially block other calls from reaching the remote-site Cisco Unified CME.

You can configure a router to act as an H.450 Cisco IP-to-IP Gateway, and use it to proxy H.450 service for the Cisco Unified CallManager, and avoid extending the hairpin call path all the way to the remote-branch Cisco Unified CME system.

Calls from the Cisco Unified CallManager to the remote Cisco Unified CME systems are configured to pass through an H.450 Cisco IP-to-IP Gateway that is co-located with the Cisco Unified CallManager at the central site. The H.450 Cisco IP-to-IP Gateway adds an H.450.12 capabilities indication to the call before it is sent to the remote Cisco Unified CME system. This allows the remote Cisco Unified CME system to invoke H.450.2 transfer or H.450.3 call forwarding on the call. The H.450 Cisco IP-to-IP Gateway intercepts any H.450.x service messages sent by the Cisco Unified CME system. If the call path required by the H.450 service invocation requires a VoIP-to-VoIP hairpin, the hairpin is created at the central site, where bandwidth is more plentiful. You still get a VoIP-to-VoIP hairpin path, but the hairpin is located in the central site network instead of the call path going all the way to the remote Cisco Unified CME system at the far end of the WAN link, as shown in Figure 6-8. In this figure, the H.450 Cisco IP-to-IP Gateway provides proxy services for H.450 messages coming from the Cisco Unified CME systems. Call transfers/forwards are rolled back to the Cisco IP-to-IP Gateway instead of hairpinning the call at the remote-branch site.

Figure 6-8 H.450 Cisco IP-to-IP Gateway



Consider the case of a call from the Cisco Unified CallManager that goes through the H.450 Cisco IP-to-IP Gateway to Cisco Unified CME 1 and is then H.450.3 forwarded to Cisco Unified CME 2. For this case, the H.450.3 forwarding request causes the original call to be rolled back to the H.450 Cisco IP-to-IP Gateway and then reoriginated to the second Cisco Unified CME 2. The final call path for the forwarded call is actually optimum for this case. It's the same call path as a direct dialed call from the Cisco Unified CallManager to Cisco Unified CME 2. The physical IP packet path for the call is the same as you would get for a pure H.450.3 case.

Furthermore, the router you deploy to act as the H.450 Cisco IP-to-IP Gateway can also be equipped with physical voice ports. It then can do double duty and act as a PSTN gateway to provide central PSTN access for the Cisco Unified CallManager and also, optionally, for the remote Cisco Unified CME systems.

To configure a router to act as an H.450 Cisco IP-to-IP Gateway, you simply create VoIP dial peers to direct incoming VoIP calls to outgoing VoIP links, as shown in the following example.

```
voice service voip
       supplementary-service h450.12
       allow-connections h323 to h323
```

The same caveats that apply to Cisco Unified CME hairpin routing also apply in the H.450 Cisco IP-to-IP Gateway case. The inbound and outbound VoIP call legs need to use the same codec unless you use a DSP farm to provide transcoding.

In the case that you use an H.450 Cisco IP-to-IP Gateway to also provide PSTN access, you may need to configure separate dial peers to allow the central site Cisco Unified CallManager-to-PSTN calls to operate using G.711 at the same time Cisco Unified CallManager-to-Cisco Unified CME via Cisco IP-to-IP Gateway calls
use G.729.

Integrating Cisco Unified CME in a SIP Network

Much of what you have read about linking Cisco Unified CME systems over WAN VoIP links for H.323 also applies to SIP, so a lot of the heavyweight detail that's been covered for H.323 is not repeated here. Instead, the following sections focus on some of the differences between SIP and H.323 implementations. This approach also helps you understand some of the issues associated with investment

protection for your VoIP network and hopefully provides some reassurance about picking the "right" protocol for intersite calls. Cisco Unified CME provides you with flexibility and safeguards against protocol dependencies.

A major point that should be made here is that Cisco IOS software and Cisco Unified CME system support of SIP is primarily for *SIP trunking*, or using SIP as a protocol to connect calls between peer Cisco Unified CME systems over a WAN link. This is primarily a property inherited from the Cisco IOS Voice Infrastructure functionality that underlies Cisco Unified CME. This is quite a different usage case than that of connecting SIP phones directly to Cisco Unified CME.

However, you can host SIP phones directly on Cisco Unified CME 3.0, because the same Cisco IOS Release 12.3(4)T also independently includes the Survivable Remote Site Telephony for SIP (SIP-SRST) feature that provides a basic Registrar and Redirect Server. The services and features that you can access from the SIP phones are very limited in comparison to the phone features offered for SCCP-based phones. More significantly, Cisco Unified CME 3.x does not provide any mechanisms to support administration and configuration management for SIP phones.

You can also host H.323-based phones on a Cisco Unified CME system if you use a router image that includes gatekeeper functionality. These services that enable support of H.323 and SIP phones are part of the general Cisco IOS Voice Infrastructure functionality and are unrelated to Cisco Unified CME.

You should understand here that although you can concurrently and independently operate the IOS Voice SIP and H.323 phone-hosting capabilities with Cisco Unified CME, this functionality is not integrated and productized in the same way as support for SCCP phones. Cisco Unified CME 3.0, 3.1, and 3.2 are not marketed as providing SIP or H.323 phone support for this reason.

The following sections describe using SIP to interconnect Cisco Unified CME systems:

Two-Node Topology with SIP

You can connect two Cisco Unified CME systems using a pair of VoIP dial peers configured symmetrically on each Cisco Unified CME to point to the other Cisco Unified CME. This is exactly the same as the H.323 case described in "A Simple Two-Node Topology with H.323" section on page 6-5. The only difference is that you must explicitly select SIP in your dial peer, whereas H.323 is the default protocol.

For a pair of Cisco Unified CME systems that have extensions 1000 to 1099 on Cisco Unified CME 1 (IP address 10.1.1.1) and 2000 to 2099 on Cisco Unified CME 2 (IP address 10.1.2.1), you need the dial peers shown in the following example:

- Cisco Unified CME 1

```
dial-peer voice 2000 voip
     destination-pattern 20..
     session target 10.1.2.1
     session protocol sipv2
```

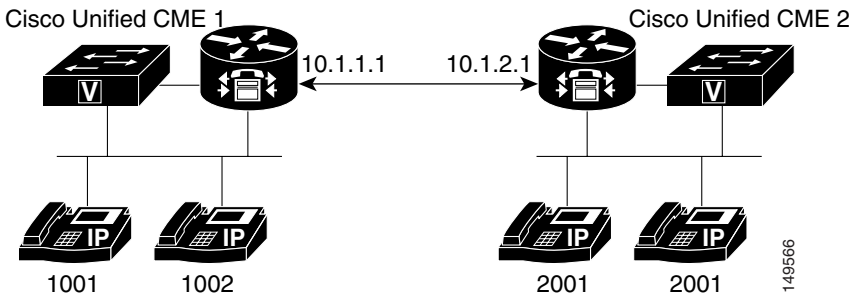
```
        dtmf-relay sip-notify
        dtmf-relay rtp-nte
        codec g729r8
        no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1000 voip
     destination-pattern 10..
     session target 10.1.1.1
     session protocol sipv2
     dtmf-relay sip-notify
     dtmf-relay rtp-nte
     codec g729r8
     no vad
```

As you can see, switching your simple two Cisco Unified CME system network from H.323 to SIP is easy. All you need to add is **session protocol sipv2** to the dial peers on both systems and it is done. You will also notice that the dtmf-relay method has been changed. Additional information about this command is provided in"DTMF Relay and RFC 2833 for SIP" section on page 6-34. Note that the sip-notify form of DTMF relay is required for Cisco Unified CME systems that use Cisco Unified CME 3.1 or earlier versions. Cisco Unified CME systems based on Cisco Unified CME 3.2 or later versions should use the **dtmf-relay rtp-nte** form where possible. See Figure 6-9.

Figure 6-9 Simple Two-Node Cisco Unified CME SIP Network



The following example shows the relevant Cisco Unified CME node configurations.

- Cisco Unified CME 1

```
dial-peer voice 2000 voip
   destination-pattern 20..
   session target ipv4:10.1.2.1
   session protocol sipv2
   dtmf-relay rtp-nte
   no vad
```

- Cisco Unified CME 2

```
dial-peer voice 1000 voip
   destination-pattern 10..
   session target ipv4:10.1.1.1
   session protocol sipv2
   dtmf-relay rtp-nte
   no vad
```

You face exactly the same issues and options as in the H.323 case in expanding beyond a two-node H.323 Cisco Unified CME network to a multinode SIP network. The exception is that Cisco Unified CME does not natively support Cisco IP-to-IP Gateway SIP call routing. However, you can easily buy another company's SIP proxy or redirect server to do this instead.

SIP Proxy/Registrar/Redirect Server

In H.323 you saw how you can use an H.323 gatekeeper to provide telephone number-to-IP address resolution. In SIP this same function is often carried out using a SIP registrar and a SIP Redirect Server that are internally linked. The SIP Registrar accepts SIP REGISTER messages from client voice endpoint systems (called user agents [UAs] in the SIP world) and uses them to build a phone number-to-IP address conversion database. Just as Cisco Unified CME can generate H.323 gatekeeper registrations, Cisco Unified CME can generate SIP REGISTER messages based on the Cisco Unified CME ephone-dn extension numbers and **dialplan-pattern** command. Cisco Unified CME can maintain concurrent registrations with both an H.323 gatekeeper and SIP Registrar at the same time.

There is a small difference in the protocol flow between the H.323 and SIP cases. In the H.323 case, an explicit address query (ARQ) goes from the Cisco Unified CME to the gatekeeper to obtain the destination IP address from the destination phone number. As soon as that operation is successful, the Cisco Unified CME initiates a call setup. In the SIP case the Cisco Unified CME sends an INVITE call setup message to the combined SIP Registrar/Redirect Server. The Redirect Server responds with a REDIRECT message that guides the Cisco Unified CME to send a second INVITE message to the correct IP address.

The combination of a Registrar and Redirect Server in a single system is often called a *SIP proxy*, albeit a very basic one. In an alternative implementation, the proxy accepts the initial INVITE sent by the Cisco Unified CME. Instead of responding with a redirect response, the proxy may simply relay the INVITE to its final destination. This is similar to Cisco IP-to-IP Gateway call routing and to the action of a routed signaling gatekeeper in the H.323 context.

To use the services of a SIP proxy with your VoIP dial peers, you can use the configuration shown in the following example.

```
sip-ua
       sip-server ipv4:10.1.10.2
dial-peer voice 408525 voip
       destination-pattern 408525....
       session target sip-server
       dtmf-relay rtp-nte
       no vad
```

You can use a DNS name instead of a raw IP address for the sip-server address.

To register your Cisco Unified CME phone numbers with an external SIP registrar, you can use the configuration shown in the following example.

```
sip-ua
 authentication username user1 password 12345 realm domain
 no remote-party-id
 registrar dns:10.1.10.2 expires 3600
```

Note that the authentication command authenticates against the SIP registrar. In order for extensions to register to the SIP registrar, each must successfully authenticate.

Public and Internal Phone Numbers in a SIP Network

Just as for H.323, you may need to choose which phone numbers you register with a SIP registrar. You can control this in the same way that you learned for H.323 using the **dialplan-pattern** command and the **no-reg** option for the **ephone-dn number** command.

Although SIP does allow the use of Internet domain names for telephone number scoping purposes, this is not supported by the IOS SIP Voice Gateway software. The IOS SIP Voice Gateway software mostly ignores domain names in SIP messages.

DTMF Relay and RFC 2833 for SIP

The same technical issues and motivations exist for DTMF relay in SIP as in H.323. The first-choice DTMF relay method for most SIP networks is the RTP-based RFC 2833 protocol. Unfortunately, the Cisco SCCP IP phones do not natively support this.

As you saw in"DTMF Relay for H.323" section on page 6-17, the Cisco SCCP phones only provide out-of-band control channel signaling for DTMF digits. In the H.323 world, this can be easily translated into H.245 alphanumeric signaling events to pass across VoIP over WAN.

The equivalent method in the SIP domain is to use a SIP NOTIFY event. However, this is not well standardized. The original SIP DTMF NOTIFY implemented in the Cisco IOS Voice Gateway software is based on an early draft proposal for this mechanism and, therefore, is not supported on most third-party SIP products. However, this mechanism is adequate provided that you are using only Cisco IOS voice endpoints with Cisco IOS Release 12.3(4)T or later. You also need to transport DTMF keypad events across VoIP to an IOS PSTN voice gateway for regeneration as an audio signal into a PSTN trunk or FXS port.

To enable the SIP NOTIFY for dtmf-relay, add the following command to your SIP VoIP dial peers:

dtmf-relay sip-notify

Cisco Unified CME 3.2 introduces support for conversion and interworking between the SCCP control channel DTMF digit indications and RTP-based RFC 2833 (for SIP only). This significantly improves the Cisco Unified CME system's ability to work with SIP networks that include another company's SIP-based voice mail systems. To use this RFC 2833 RTP in-band to SCCP out-of-band interworking function for dtmf-relay, you use the following:

dtmf-relay rtp-nte

Note Cisco Unity Express 2.2 and earlier versions support only the **sip-notify** format of DTMF relay. When using Cisco Unity Express 2.2 or earlier versions, youmust use **sip-notify** on the SIP VoIP dial peers used to interconnect Cisco Unified CME with Cisco Unity Express. Even when using the notify method in the SIP VoIP dial peers for interworking with Cisco Unity Express, you can simultaneously use the RFC 2833 mechanism on other SIP VoIP dial peers that require it. Cisco Unity Express 2.3.1 and later support RFC 2833. For these versions, you can use RFC2833 **dtmf-relay rtp-nte** on the SIP VoIP dial peers used to interconnect Cisco Unified CME with Cisco Unity Express.

We recommend using of RFC 2833 **dtmf-relay rtp-nte** for SIP when possible.

Note Cisco Unified CME does not support raw, in-band DTMF which is the implementation used by some SIP service providers. If these situations, Cisco Unified CME IP phones will not be able to send DTMF to the SIP cloud and inbound calls terminated on the Cisco Unified CME will not be able to receive DTMF. The SIP service provider to which the Cisco Unified CME connects must either support RFC 2833 or SIP-notify in order for DTMF to operate properly.

SIP Supplementary Services

The SIP supplementary services for call transfer and call forwarding enjoy significantly more widespread support across the majority of another company's SIP implementations compared with supplementary services for H.323. These services have been part of the SIP landscape from fairly early on in the development of SIP, in contrast with the history of H.323, where these services were defined relatively late.

The main difference between H.323 supplementary services is that SIP supplementary services (such as MWI notification, REFER, and 3XX) cannot be disabled (unlike H.450). If you connect a Cisco Unified CME to a SIP service provider that does not support these service, then call forwards and transfers invoked by the Cisco Unified CME will fail.

MWI Notification

Message waiting indicator (MWI) notification is a SIP supplementary service that enables outcall-based Cisco Unified CME support of Subscribe/Notify and unsolicited notify functions for receiving MWI over SIP. Key capabilities include the ability to:

- Generate unsolicited notify messages to SIP endpoint for outcall
- Subscribe to MWI server for SIP endpoint
- Relay unsolicited notify messages to SIP endpoints for unsolicited notify and subscribe/notify
- Support unsolicited notify internetworks with MWI Relay

Several MWI notification examples follow:

- MWI notification outcall configuration example

```
ephone-dn1
  number 9000...
  mwi on-off
```

  In the preceding example, the number 9000... command defines the MWI callback pilot number.

- Unsolicited notify configuration example

```
sip-ua
  mwi-server ipv4:10.5.49.200 unsolicited
voice register dn 1
  number 1234
  mwi
```

  In the preceding configuration example, the **mwi-server** command defines the unsolicited MWI server and the standalone **mwi** command specifies extension support.

- Subscribe/notify configuration example

```
sip-ua
  mwi-server ipv4:10.5.49.200
```

```
voice register dn 1
  number 1234
  mwi
```

In the preceding configuration example, the **mwi-server** command defines the subscribe/notify MWI server.

SIP REFER

Call transfer with SIP is supported using the SIP REFER method. As its name suggests, it allows one SIP UA, or endpoint, to refer a caller to a different SIP UA. It operates in a similar way to H.450.2. It triggers a replacement of the transferor-to-transfer-to consultation call by a transferee-to-transfer-to call. Just as in the H.450.2 case, the original and consultation call legs are treated as unrelated and independent entities until the call transfer is actually committed. Just like H.450.2, three possible transfer scenarios exist:

- Transfer-consult with commit-at-connect
- Transfer-consult with commit-at-alerting
- Blind transfers (without any consultation call)

One difference is that there is no specific consultation ID exchange transaction between the transferor and transfer-to parties, because SIP inherently contains a mechanism to uniquely identify the call being replaced at the transfer-to endpoint.

For the sake of completeness in describing SIP transfers, an older (and less preferred) SIP method called BYE/ALSO exists for executing blind transfers with SIP. As its name suggests, this is a method whereby the transferor terminates the original call from the transferee (BYE) but includes a request in the termination for the transferee to generate a follow-on call (to the transfer-to destination) using the ALSO part. Cisco Unified CME does not use the BYE/ALSO method to initiate transfers, but it does support receipt of this method from other SIP devices. This is the method used by the automated attendant (AA) in Cisco Unity Express.

To enable Cisco Unified CME to send REFER messages for call transfers, you need to configure **transfer-system full-consult** under **telephony-services**. This is the same basic configuration that is needed for H.450.2 transfers.

Unlike the H.450.2-related IOS CLI, there are no configuration commands to directly control usage of the REFER mechanism. This is a reflection of the almost-universal support that exists for REFER. There is little need to be able to enable and disable it in the same way as H.450.2.

SIP 3XX Response

Call forwarding in SIP is supported mostly using the 302 moved temporarily in response to an incoming SIP call setup INVITE message. Just like the H.450.3 protocol, this response includes the alternate forward-to destination information (phone number). It requests that the caller cancel the original call and create a new call to the indicated destination. A range of SIP responses in the 3xx value code range includes a 300 multiple-choice response that allows the forwarding party to provide the caller with a range of alternative contacts. The 300-response code is not directly supported in the Cisco Unified CME context. However, the Cisco IOS voice router SIP-SRST feature can generate this under some circumstances that are a little outside the scope of this book. You can find more information on this on Cisco.com by searching for “SIP Survivable Remote Site Telephony” under the *Cisco Unified SRST 3.2 Feature Guides*.

To enable call forwarding using the 302 response, you need to configure **call-forward pattern .T** under the **telephony-services** command. This is the same basic configuration that is used for H.450.3 call forwarding.

Like the REFER case, no commands in Cisco IOS software specifically control the generation of the 302 response because of the universal support of this message by another company's SIP devices.

SIP Interoperability

Interoperability for basic calls and transfer and forwarding for SIP is generally widespread among multiple SIP offerings from Cisco and another company's products. The one major caveat for this with Cisco Unified CME 3.0 and 3.1 is the lack of RFC 2833 support for DTMF relay. This is solved with Cisco Unified CME 3.2.

SIP is undergoing very rapid evolution, and many Internet Engineering Task Force (IETF) RFC drafts are in circulation at any given time. This is a good news/bad news situation. On the plus side, it shows that SIP is a flexible and extensible protocol. On the minus side, this situation has a lot of the larger and more conservative VoIP customers in a mode where they are waiting to see some stability before going to large, widespread deployments. By their very nature, large-scale deployments have difficulty absorbing significant and rapid protocol churn. If 100,000 endpoints are deployed in a VoIP network, it is very hard to do frequent upgrades to absorb the latest and greatest new protocol features.

Because Cisco Unified CME is based on top of the H.323 and SIP software that is part of the Cisco IOS Voice Gateway code, Cisco Unified CME automatically keeps up with, and benefits from, the best of both protocols. It represents a low-risk approach to VoIP telephony.